НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
Кафедра інформаційної безпеки

«На правах рукопису»
УДК _____

«До захисту допущено»
В.о. завідувача кафедри
_____
М.В.Грайворонський
“___”_____2018 р.

Магістерська дисертація

на здобуття ступеня магістра

зі спеціальності: 125 Кібербезпека

на тему: Модель системи захисту інформації для хмарної СКБД

Виконала: студентка 6 курсу, групи ФБ-71мп
(шифр групи)

Мазуренко Анастасія Євгенівна _____
(прізвище, ім’я, по батькові) (підпис)

Науковий керівник доцент кафедри ІБ, к.т.н. Коломицев Михайло Володимирович
(посада, науковий ступінь, вчене звання, прізвище та ініціали)
_____
_____
(підпис)

Консультант _____ _____ _____
(назва розділу) (науковий ступінь, вчене звання, , прізвище, ініціали) (підпис)

Рецензент _____ _____
(посада, науковий ступінь, вчене звання, науковий ступінь, прізвище та ініціали) (підпис)

Засвідчую, що у цій магістерській дисертації немає запозичень з праць інших авторів без відповідних посилань.
Студент _____
(підпис)

Київ – 2018 року

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
Кафедра інформаційної безпеки

Рівень вищої освіти – другий (магістерський) за освітньо-професійною програмою
Спеціальність (спеціалізація) – 125 Кібербезпека (« Системи і технології Кібербезпеки »)

ЗАТВЕРДЖУЮ
В.о. завідувача кафедри
_____ М.В.Грайворонський
(підпис)
«___»_____2018 р.

ЗАВДАННЯ
на магістерську дисертацію студенту

_____
(прізвище, ім'я, по батькові)

1. Тема дисертації Модель системи захисту інформації для хмарної СКБД,
науковий керівник дисертації к.т.н. Коломицев Михайло Володимирович ,
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
затверджені наказом по університету від «15» листопада 2018 р. № 4171-с
2. Термін подання студентом дисертації 12.12.2018 р.
3. Об'єкт дослідження: технології та засоби забезпечення захисту інформаційних ресурсів хмарних сервісів для зберігання та обробки даних.
4. Вихідні дані:
5. Перелік завдань, які потрібно розробити:
    1. аналіз документації, що регламентує сферу застосування хмарних технологій, класифікацію інформації, захист даних в СКБД;
    2. аналіз вимог що до захисту інформації відповідно до її класифікації;
    3. аналіз класифікації та архітектури хмарних сервісів, аналіз вразливостей та загроз;
    4. аналіз та систематизація одержаних результатів;
    5. побудова власної моделі системи захисту даних в хмарних СКБД.

6. Орієнтовний перелік ілюстративного матеріалу 15 слайдів

7. Орієнтовний перелік публікацій 1 публікація

8. Консультанти розділів дисертації*

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

9. Дата видачі завдання _____

Календарний план

№ з/п	Назва етапів виконання магістерської дисертації	Термін виконання етапів магістерської дисертації	Примітка
1.	Узгодження теми		
2.	Аналіз документації, що регламентує сферу застосування хмарних технологій, класифікацію інформації, захист даних в СКБД		
3.	Аналіз вимог що до захисту інформації відповідно до її класифікації		
4.	Аналіз класифікації та архітектури хмарних сервісів, аналіз вразливостей та загроз		
5.	побудова власної моделі системи захисту даних в хмарних СКБД		

Студент _____ _____
(підпис) (ініціали, прізвище)

Науковий керівник дисертації _____ _____
(підпис) (ініціали, прізвище)

* Консультантом не може бути зазначено наукового керівника магістерської дисертації.

РЕФЕРАТ

Робота об’ємом ### сторінок, яка містить ### ілюстрацій, 13 таблиць, ### джерел за переліком посилань та ### додатки.

Метою даної кваліфікаційної роботи є розробка моделі системи захисту інформації для хмарної системи керування базами даних, яка дасть можливість побудови системи захисту інформації для хмарних систем керування базами даних та забезпечення належного рівня безпеки даних, що зберігаються та оброблюються в таких системах.

Об’єктом дослідження є технології та засоби забезпечення захисту інформаційних ресурсів хмарних сервісів для зберігання та обробки даних.

Предметом дослідження є забезпечення належного рівня захисту інформації в хмарних системах керування базами даних.

Методом дослідження є опрацювання літератури та інших інформаційних джерел за даною темою, розгляд міжнародних стандартів та інших документів, що регулюють галузь хмарних обчислень, аналіз існуючих методів та засобів захисту інформації та їхніх характеристик, аналіз вимог що до захисту інформації при зберіганні та обробці в хмарних системах керування базами даних.

Результати роботи можуть бути використані для побудови системи захисту інформації, застосовної до хмарних систем керування базами даних.

ІНФОРМАЦІЙНА БЕЗПЕКА, ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ, ХМАРНІ ОБЧИСЛЕННЯ, ХМАРНІ СИСТЕМИ КЕРУВАННЯ БАЗАМИ ДАНИХ, ЗАХИСТ ІНФОРМАЦІЇ

РЕФЕРАТ

Работа объемом ### страниц, содержащая ### иллюстраций, ### таблиц, ### источников по перечню ссылок и ### приложения.

Целью данной квалификационной работы является разработка модели системы защиты информации для облачной системы управления базами данных, которая даст возможность построения системы защиты информации для облачных систем управления базами данных и обеспечения надлежащего уровня безопасности данных, хранящихся и обрабатываемых в таких системах.

Объектом исследования являются технологии и средства обеспечения защиты информационных ресурсов облачных сервисов для хранения и обработки данных. Предметом исследования является обеспечение надлежащего уровня защиты информации в облачных системах управления базами данных.

Методом исследования является обработка литературы и других информационных источников по данной теме, рассмотрение международных стандартов и других документов, регулирующих сферу облачных вычислений, анализ существующих методов и средств защиты информации и их характеристик, анализ требований к защите информации при хранении и обработке в облачных системах управления базами данных.

Результаты работы могут быть использованы для построения системы защиты информации, применимой к облачным системам управления базами данных.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ, ОБЛАЧНЫЕ ВЫЧИСЛЕНИЯ, ОБЛАЧНЫЕ СИСТЕМЫ УПРАВЛЕНИЯ БАЗАМИ ДАННЫХ, ЗАЩИТА ИНФОРМАЦИИ

ABSTRACT

Work with ### pages containing ### illustrations, ### tables, ### sources by list of links and ### attachments.

The purpose of this qualification work is to develop an information security system model for cloud database management system that enable the design of a data protection system for cloud-based database management systems and provide an adequate level of data security that is stored and processed in such systems.

The object of the research is the technologies and means of ensuring the protection of information resources of cloud services for storage and processing of data.

The subject of the study is to provide an adequate level of information security in cloud-based database management systems.

The research method is the analysis of literature and other information sources on this topic, consideration of international standards and other documents regulating cloud computing, analysis of existing methods and means of protecting information and their characteristics, analysis of information security requirements for storage and processing in cloud management systems databases.

The results of the work can be used to build a data protection system in cloud-based database management systems.

INFORMATION SECURITY, INFORMATION TECHNOLOGIES, CLOUD CALCULATIONS, DATA BASES MANAGEMENT SYSTEMS, INFORMATION PROTECTION

ЗМІСТ

Перелік умовних позначень, символів, одиниць, скорочень і термінів 9
Вступ 10
1 Аналіз предметної області 13
1.1 Концепція хмарних технологій 13
1.2 Класифікація хмарних сервісів 14
1.3 Архітектура хмарної інфраструктури 25
1.4 База даних як сервіс 38
Висновки до розділу 1 43
2 Методи та засоби захисту інформації в хмарних скбд 44
2.1 Нормативно-правова документація, що врегульовує сферу захисту інформації 44
2.2 Аналіз інформаційної безпеки 46
2.2.1 Загрози 47
2.2.2 Атаки на хмарні сервіси та рішення щодо їх усунення 51
2.3 Структура моделі системи захисту інформації 54
2.3.1 Захист каналів зв’язку 54
2.3.2 Автентифікація та авторизація користувачів 62
2.3.3 Політики безпеки 71
2.3.4 Моніторинг та аудит 78
2.3.5 Криптографічний захист даних 79
2.3.6 Обробка шифрованих даних у скбд 80
Висновки до розділу 2 84
3 Модель захисту даних для хмарних скбд 85
висновки 112
4 Аналіз виходу на ринок стартап проекту 113
4.1 Опис ідеї стартап проекту 113
4.2 Технологічний аудит ідеї проекту 117
4.3 Аналіз ринкових можливостей запуску стартап проекту 120
4.4 Розроблення маркетингової програми 121
4.5 Розроблення ринкової стратегії проекту 130

4.6 Розроблення маркетингової програми стартап-проекту 133
Перелік посилань 136

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

API – програмний інтерфейс застосунку

CSP (Content security policy) – політика захисту контенту

DBaaS – база даних як послуга

IaaS – інфраструктура як послуга

PaaS – платформа як послуга

PII (Personally identifiable information) – персональні дані ідентифікації

SaaS – програмне забезпечення як послуга

SLA – угода про рівень послуг

АС – автоматизована система

НСД – несанкціонований доступ

ОС – операційна система

ПЗ – програмне забезпечення

СЗІ – система захисту інформації

СКБД – система керування базами даних

ВСТУП

Інформаційні ресурси відіграють дуже суттєву роль в сучасних реаліях, оскільки все більше розширюються межі їх використання та коло користувачів, що мають доступ до інформаційної системи, в якій дані ресурси зберігаються та обробляються, збільшуються обсяги інформації, що підлягає обробці та зберіганню в електронному форматі, зростає цінність, яку вони ставлять для власників (приватних осіб, організацій і т.д.), а отже, і роль даних як ресурсу у конкурентній боротьбі дедалі зростає. Розвитку також набувають методи та засоби автоматизації процесів зберігання та обробки інформації, так як з'являється необхідність надання доступу різних рівнів багатьом користувачам до однієї інформаційної системи, забезпечуючи при цьому цілковиту безпеку ресурсів як при транспортуванні даних, так і при їх обробці на зберіганні.

Разом з цим невід'ємно зростає і спектр вразливостей, які можуть бути виявлені в даних інформаційних системах, а також загроз, що можуть експлуатувати дані вразливості. Таким чином, в зв'язку зі стрімким поширенням використанням технологій для зберігання та обробки інформації питання про забезпечення безпеки інформації і, відповідно, створення стійкої СЗІ є не менш важливим, ніж створення та забезпечення стабільної роботи самих систем обробки та зберігання даних.

Окремої популярності набуває використання хмарних сервісів як для проведення різноманітних обчислень будь-якого ступеню складності, так і для нескладної обробки і зберігання даних різного об'єму. Це є зручним для користувача, оскільки йому в користування надається високопродуктивна та відмовостійка віртуальна інфраструктура, що надає можливість швидкої та безпечної обробки даних, але при цьому не треба вкладати кошти та зусилля в закупівлю дорогого обладнання, його обслуговування, налаштування, та, найголовніше - в забезпечення належного рівня безпеки інформаційних ресурсів. Провайдери хмарних сервісів, в свою чергу, відповідають за безпеку ресурсів,

надання необхідних обчислювальних потужностей та забезпечують доступність даних для клієнта. Доступ до інформації, що розміщено та зберігається в хмарі, надається через типові протоколи зберігання даних або ж напряму через програмний інтерфейс застосунку (API).

Питання захисту інформації для будь-якої системи, яка працює з інформацією, що має певну комерційну значимість, є невід'ємним атрибутом. Доступ підприємства (або окремого користувача) до хмари піднімає проблеми захищеності інформації, яка проходить через зовнішню мережу (інтернет), та обмеження доступу зовнішніх користувачів до внутрішньої мережі. Захист інформації при її обробці, зберіганні та транспортуванні – найактуальніша задача для хмарних СКБД.

Актуальність даної кваліфікаційної роботи випливає з необхідності забезпечення належного рівня захисту користувацьких даних відповідно до їхньої класифікації, при їх транспортуванні, обробці та зберіганні з використанням хмарних технологій.

Метою даної роботи є дослідження методів та засобів захисту інформації та розробка моделі системи захисту інформації для хмарних СКБД, що дозволить забезпечити належний рівень безпеки даних при оптимальному використанні ресурсів для побудови та забезпечення функціонування інформаційної системи.

Для досягнення мети було поставлено наступні завдання:

- огляд та аналіз документації, що регламентує сферу застосування хмарних технологій, класифікацію інформації, захист даних в СКБД
- аналіз вимог що до захисту інформації відповідно до її класифікації
- аналіз класифікації та архітектури хмарних сервісів, аналіз вразливостей та загроз
- аналіз та систематизація одержаних результатів
- побудова власної моделі системи захисту даних в хмарних СКБД

Об'єктом дослідження є технології та засоби забезпечення захисту інформаційних ресурсів хмарних сервісів для зберігання та обробки даних.

Предметом дослідження є забезпечення належного рівня захисту інформації в хмарних системах керування базами даних.

Методом дослідження є опрацювання літератури та інших інформаційних джерел за даною темою, розгляд міжнародних стандартів та інших документів, що регулюють галузь хмарних обчислень, аналіз існуючих методів та засобів захисту інформації та їхніх характеристик, аналіз вимог що до захисту інформації при зберіганні та обробці в хмарних системах керування базами даних.

Наукова новизна одержаних результатів полягає у використанні найбільш вдалих рішень та засобів для захисту інформації та приведення їх до спільної моделі системи захисту інформації, яка оброблюється та зберігається в хмарних СКБД.

Практичне значення результатів роботи випливає з того, що створена модель дозволить оптимізувати використання ресурсів для захисту інформації, залежно від її класифікації та забезпечити належний рівень захищеності.

Публікації:

1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ

1.1 Концепція хмарних технологій

Хмарні технології надають користувачам можливість доступу до даних та їх обробки або ж можливість використання певних сервісів через мережу, тобто відсутня необхідність локальної наявності ресурсів для зберігання та обробки інформації, а також певних застосунків або інших сервісів.

Хмарні обчислення (cloud computing) – модель для надання можливості мережевого доступу на вимогу до масштабованого та еластичного розподіленого пулу конфігурованих фізичних або ж віртуальних ресурсів спільного використання за принципом самообслуговування та адмініструванням за вимогою.

Сервіс хмарних обчислень (cloud service) – можливості, які надаються за допомогою хмарних обчислень, викликається через певний інтерфейс.

Основні види послуг, що надаються провайдерами хмарних рішень, поділяються на надання через технології мережевого доступу обчислювальних потужностей, дискового простору або ж певних сервісів, таких як використання застосунків. Така концепція надання послуг має ряд беззаперечних переваг, оскільки раціоналізує використання ресурсів користувачами, так як в них відсутня необхідність купівлі, утримання та захисту власних серверів, забезпечення необхідних обчислювальних потужностей, розгортання та підтримання комп’ютерної інфраструктури, а також в локальної наявності та підтримки застосунків та інших сервісів. Таким чином, користувач сплачує лише за ті ресурси, які безпосередньо використовує, наприклад, не купує обладнання та спеціальне програмне забезпечення для проведення певних складних операцій, коли більшу частину часу воно не використовуватиметься, а орендує його в провайдерів саме для виконання конкретного обсягу або задачі, не переплачуючи при цьому за локальну наявність та утримання обчислювальних або інших

ресурсів. Провайдер при цьому забезпечує повсюдну доступність інформації або ресурсів на вимогу за використанням мережевих технологій , можливість гнучкого масштабування.

Однак, є також і ряд речей, які не можна однозначно ідентифікувати як недоліки даного підходу, але які потребують особливої уваги для уникнення небажаних ситуацій:

– доступ до даних або сервісів надається за використанням мережевих технологій, тобто доступ до ресурсів буде неможливим без Інтернет підключення;
– узгодження умов надання послуг з провайдером – провайдери можуть заблокувати доступ на деякий час або видалити дані в разі невчасної сплати, якщо таке передбачено умовами договору;
– конфіденційність користувацьких даних забезпечує провайдер, тому, при відсутності відповідних пунктів у договорі, їх недотриманні або інцидентах в сфері інформаційної безпеки – конфіденційність даних (або й інші характеристики) може бути порушена.

1.2 Класифікація хмарних сервісів

З огляду на те, що хмарні сервіси представлені цілим набором різноманітних послуг, першочергово слід зазначити ряд їхніх основних характеристик, притаманних всім типам даної парадигми.

Ключові характеристики хмарних сервісів:

1. Широкий мережевий доступ (Broad network access) – фізичні та віртуальні ресурси доступні через мережу за допомогою застосування стандартних механізмів, що дає змогу організувати взаємодію з різноманітними клієнтськими платформами. Це забезпечує можливість отримання доступу користувачами до фізичних або віртуальних ресурсів з будь-якого місця та пристрою.

2. Вимірюване обслуговування (Measurable service) – можливість управління використанням послуги на основі певних критеріїв та за допомогою певних засобів вимірювання. Дана характеристика також відкриває можливості моніторингу та оптимізації, а також перевірки коректності надання хмарного сервісу. З іншого ж боку, користувач при цьому сплачує за сервіс у відповідності з його використанням, при цьому отримуючи можливість переходу від низько-ефективної бізнес-моделі використання активів до високо-ефективної. При цьому, хмарні сервіси оптимізують контроль ресурсів за допомогою засобів вимірювання, а також забезпечується повна прозорість цього процесу як для постачальника, так і для користувача.
3. Самообслуговування на вимогу (On-demand self-service) – можливість доступу споживача до наданих ресурсів автоматично без взаємодії з постачальником послуг, тобто в односторонньому порядку. Таким чином, це забезпечує можливість користувачам до скорочення витрат, часу та зусиль.
4. Миттєва еластичність та масштабованість (Rapid elasticity and scalability) – здатність фізичних та віртуальних ресурсів до швидкої та гнучкої адаптації до потреб клієнта щодо збільшення або зменшення кількості необхідних до використання ресурсів. У відповідності до обмежень угоди про надання послуг (Service Level Agreement) ресурси можуть також надаватись в необмеженій кількості в будь-який час в залежності від потреби та, в більшості випадків, адаптація об’єму \ потужності виділюваних ресурсів проводиться автоматично, що дозволяє клієнту не виконувати процес планування необхідних обчислювальних потужностей та дискового простору. Також за рахунок автоматизації процедур перерозподілу виділених ресурсів суттєво знижуються витрати на обслуговування абонентів.
5. Пул ресурсів (Resource pooling) – об’єднання фізичних та віртуальних ресурсів постачальника хмарних сервісів для обслуговування одного або

групи клієнтів, таким чином постачальник має змогу підтримувати багатокорстувальницьку модель обслуговування клієнтів (які мають різні потреби в виділяємих фізичних або віртуальних ресурсах), надаючи клієнтам абстракції, при цьому клієнти не керують розподіленням ресурсів та не знають реальної складності процесів розподілення до найвищого рівня абстракції. Вимоги до підтримки функціонування ресурсу повністю забезпечуються постачальником.

Таким чином, в зв'язку з непостійним характером споживання ресурсів споживачами, об'єднання постачальником ресурсів для обробки користувацьких даних у пули дозволяє зменшити використання апаратних ресурсів, на відміну від ситуації, коли обчислювальні потужності надаються кожному користувачу окремо.

Аспекти хмарних сервісів

Аспекти хмарних сервісів – це основні властивості, які притаманні даним сервісам, мають безперервно виконуватись та координуватись за допомогою визначених ролей, таких як споживач, партнер (відповідальний за підтримку сервісу або є допоміжною стороною по відношенню до виконання операцій постачальника хмарних обчислень, споживача, або обох сторін одночасно), постачальник хмарних сервісів.

Ключові аспекти:

- Доступність (Availability) – властивість сервісу бути доступним та застосовним на вимогу авторизованого суб'єкта (користувача).
- Продуктивність (Performance) – набір функцій, що складають операційні можливості сервісу та мають певні метрики, визначені в угоді про рівень надання послуг (SLA).
- Рівні обслуговування (Service levels) – визначаються в угоді про рівні обслуговування між постачальником послуг та споживачем на основі визначених термінів з ціллю встановлення якості послуг, що забезпечуються провайдером хмарних сервісів. Базуються на

вимірюваних характеристиках, визначених для хмарних сервісів та детермінованому наборі ролей.

- Функціональна сумісність (Interoperability) – забезпечення для користувача можливості обміну даними з постачальником послуг та отримання при цьому передбачуваних результатів.
- Керованість (Governance) – забезпечення постачальником раціонального розподілу користувацьких ресурсів та здійснення визначених угодою про надання послуг операцій над ними.
- Управління версіями та обслуговування (Versioning and maintenance) – відповідне маркування версій, прозоре та зрозуміле для користувача, підтримка контролю версій.
- Портативність (Portability) – можливість перенесення користувацьких даних або застосунків між платформами різних постачальників хмарних послуг з мінімальними затратами та належним чином (без порушень), відповідно до класифікації користувацьких даних та збереженням їхніх властивостей.
- Регулювання (Regulatory) – відповідність операцій, виконуваних постачальником над користувацькими даними, діючому законодавству, міжнародним та регіональним стандартам, регламентуючим документам, вимогам користувача і т.д.
- Здатність до відновлення (Resiliency) – здатність системи до підтримання певного обумовленого рівня надання послуг при наявності певних несправностей.
- Зворотність (Reversibility) – можливість відновлення користувацьких даних після збоїв та можливість видалення постачальників всіх даних та пов’язаних з ними артефактів сервісів після закінчення певного періоду, визначеного в угоді про рівень надання послуг.
- Безпека (Security) – забезпечення вимог безпеки, таких як наявність захисних механізмів аутентифікації та ідентифікації, доступність, конфіденційність, цілісність, відмовостійкість, аудит, моніторинг подій

безпеки, реагування на інциденти та управління політиками безпеки. Включає як фізичну безпеку носіїв цифрових даних, так і інформаційну безпеку в цифровому середовищі.

– Захист персональних даних (Protection of Personally Identifiable Information) – належний збір, обробка, транспортування, зберігання та знищення користувацьких даних, класифікованих як персональні.

Поєднання даних аспектів та характеристик хмарних сервісів є вирішальним при виборі щодо використання подібної категорії сервісів. Ці показники можуть бути використанні для аналізу доцільності раціоналізації процесів зберігання та обробки даних, планування дискового простору та обчислювальних потужностей шляхом їх перенесення на постачальників хмарних послуг, з урахуванням категоризації користувацьких даних та вимог стосовно забезпечення належного рівня захисту інформації.

Типи можливостей хмарних сервісів за функціональними можливостями, які вони надають, поділяються на:

1. Тип можливостей інфраструктури (Infrastructure-as-a-Service, IaaS) – споживачу у використання надаються ресурси для зберігання та обробки даних, або ж мережі, а також інші властивості інфраструктури для розгортання та запуску будь-яких (власних або ж придбаних) програмних застосунків, а також операційних систем. При цьому споживач не має змоги управління та контролю базової інфраструктури хмарного сервісу, але має контроль над встановленими на ньому операційними системами, сховищами даних, розгорнутими застосунками. Можлива наявність у споживача сервісу певного обмеженого контролю над обраними мережними компонентами;
2. Тип можливостей застосунку (Software-as-a-Service, SaaS) – можливість використання користувачем застосунків постачальника, які розгорнуто на хмарній інфраструктурі. Дані застосунки доступні для будь-яких тонких клієнтських інтерфейсів споживача (web-браузер або ж програмний інтерфейс). При цьому у споживача повністю відсутня

можливість здійснення управління та контролю базової інфраструктури хмарного сервісу, включаючи мережу, сервери, сховища даних, операційні системи, окремі можливості застосунків, за винятком їх специфічних конфігураційних параметрів;

3. Тип можливостей платформи (Platform-as-a-Service, PaaS) – можливість використання платформи постачальника для розгортання застосунків користувача (як власних, так і придбаних), їх запуску та управління ними, з використанням однієї або декількох мов програмування та середовищ виконання, бібліотек, а також інших послуг та інструментів, підтримка яких також забезпечується постачальником послуг. При цьому споживач не має змоги управління та контролю базової інфраструктури хмарного сервісу, включаючи мережі, сервери, операційні системи та сховища даних, але має можливість контролю над розгорнутими на даній платформі застосунками і, можливо, над деякими параметрами конфігурації середовища хостингу.

Дані три основні типи можливостей надання послуг формують фундаментальну SPI-модель. На основі виділених типів можливостей базуються категорії хмарних сервісів в залежності від послуг, які вони надають. Кожна з категорій може включати як можливості одного типу, так і їх комбінації.

Особливості типів можливостей хмарних сервісів

В рамках детермінованих типів можливостей хмарних сервісів кожен з типів обслуговування SPI має свої особливості. В першу чергу вони різняться функціональними можливостями та вимогами безпеки.

Software-as-a-Service: забезпечує більшість вбудованих функціональних можливостей, а також високий рівень безпеки з найменшою можливістю до масштабування для споживача.

Platform-as-a-Service: надає більшу масштабованість, ніж SaaS, що дає можливість для розробників створювати застосунки та контролювати дані на базі платформи. Однак, це призводить до зменшення інтегрованих функцій безпеки.

Infrastructure-as-a-Service забезпечує найбільшу масштабованість для споживачів. Це, в свою чергу, призводить до зменшення доступних інтегрованих функцій безпеки в межах захисту самої інфраструктури. Дана модель вимагає, щоб управління і захист операційних систем, програмних застосунків та контенту здійснювалось споживачем хмарних послуг.

Категорії хмарних послуг

- Інфраструктура як послуга (Infrastructure-as-a-Service, IaaS) – відповідає типу можливостей інфраструктури.
- Програмне забезпечення як послуга (Software-as-a-Service, SaaS) – відповідає типу можливостей застосунку.
- Платформа як послуга (Platform-as-a-Service, PaaS) – відповідає типу можливостей платформи.
- Обчислення як послуга (Computation-as-a-Service, CompaaS) – в даному випадку користувачу сервісу хмарних обчислень надаються в користування обчислювальні ресурси, що є необхідними для розгортання та виконання відповідного програмного забезпечення.
- Зберігання даних як послуга (DataStorage-as-a-Service, DSsaaS) – дана категорія сервісів хмарних обчислень надає споживачу послуг можливість використання ресурсів для зберігання даних, а також пов’язаних з цим можливостей.
- Мережа як послуга (Network-as-a-Service, NaaS) – категорія сервісів хмарних обчислень надає споживачу послуг мережевого транспортного зв'язку. Дана категорія передбачає оптимізацію розподілу ресурсів, розглядаючи мережеві та обчислювальні ресурси як єдине ціле.

Також виділяють три типи хмарних сховищ даних, які, в залежності від мети їх використання, мають певні переваги:

- **Об’єктне сховище** – має широкі можливості до масштабування і зберігання властивостей об’єктів у вигляді метаданих, що може ефективно використовуватись для розробки програмних застосунків в хмарних сервісах. Також можуть вдало використовуватись для імпорту даних з існуючих сховищ з метою аналітики, резервного копіювання або архівації.
- **Файлове сховище -** деяким програмним застосункам потрібен доступ до передачі файлів, отже, їм необхідна файлова система. Даний тип сховища часто підтримується сервером сховищ, підключеним до мережі (масштабні репозиторії контенту, середовища розробки, мультимедійні сховища або особисті каталоги користувачів).
- **Блочне сховище** - інші корпоративні застосунки, наприклад бази даних або системи планування ресурсів підприємства , часто потребують виділеному сховище з низькими затримками для кожного з вузлів. Таке сховище працює аналогічно сховищу з прямим підключенням або мережі зберігання даних. Виділяють сховище для кожного віртуального сервера і забезпечують наднизьку затримку для робочих навантажень, що вимагають високої продуктивності.

Комерційний ринок сервісів хмарних обчислень є досить динамічним і нові послуги продовжують з’являтись та реалізовуватись в в нових неформальних категоріях сервісів. Деякі найбільш перспективні категорії хмарних сервісів наведено нижче.

– База даних як послуга (DataBase-as-a-Service, DBaaS) – користувачу хмарного сервісу надається можливість використання функціональних можливостей бази даних на вимогу, при цьому налаштування та адміністрування бази даних виконується провайдером послуг.

– Робочий стіл як послуга (Workplace-as-a-Service, WaaS) – користувачу хмарного сервісу надається можливість використання віддаленого

робочого столу, включаючи можливості його формування, керування, збереження, виконання та інші відповідні можливості.

– Електронна пошта як послуга (Email-as-a-Service) – можливості, які надаються користувачу, являють собою повний функціонал поштової служби, включно з пов’язаними послугами з підтримки , такими як зберігання, передача, резервне копіювання та відновлення електронного листування.

– Ідентичність як послуга (Identity-as-a-Service) – можливості, які надаються користувачу, являються сервісом управління ідентифікацією та доступом, що може бути розширено та централізовано в існуючих операційних середовищах. Також включає надання, управління довідником та забезпечення роботи служби єдиної точки входу.

– Менеджмент як послуга (Management-as-a-Service) – включає в себе управління застосунками, активами, а також управління змінами, ресурсами та проблемами (функція служби підтримки), управління рівнем обслуговування.

– Безпека як послуга (Security-as-a-Service) – можливості, які надаються користувачу, являються сукупністю служб безпеки в інтегровану вигляді з існуючим операційним середовищем. Дана послуга може також включати ідентифікацію, антивірусний та антишпіонажний захист, виявлення проникнення та управління подіями безпеки.

Виходячи з вищенаведеної інформації, категорії сервісів хмарних обчислень та типи можливостей знаходяться у відношенні, яке відображено в Таблиці 1.1.

Слід також зазначити, що для категорій хмарних послуг можливими є будь-які комбінації типів можливостей, що надаються провайдерами хмарних сервісів.

Таблиця 1.1 – Відношення категорій та типів можливостей сервісів хмарних обчислень

Категорія сервісу	Тип можливостей		
	Інфраструктура	Платформа	Застосунок
Інфраструктура	+		
Платформа		+	
Застосунок			+
Обчислення	+		
Зберігання даних	+	+	+
Мережа	+	+	+
Обмін інформацією		+	+

Моделі розгортання хмарних сервісів

Моделі розгортання хмарних сервісів відображають можливі шляхи організації хмарних обчислень з точки зору управління та сумісного використання фізичних або ж віртуальних ресурсів.

1) Приватна хмара (Private cloud) – передбачає використання наданих ресурсів (доступу до даних, конфігурацій, застосунків, обчислювальних потужностей і т.д.) в межах однієї організації з можливістю надання доступу деякій кількості користувачів. Власником такого типу хмарного сервісу може являтись як сама організація, так і третя сторона або їх комбінація за певною визначеною угодою, яка встановлює розподал обов'язків з управління та обслуговування, а також забезпечення належного рівня безпеки. Фізичне розташвання ресурсів може бути як на території підприємства, так і за його межами.
2) Громадська хмара (Community cloud) - ресурси, призначені для використання конкретною спільнотою споживачів з організацій, що мають спільні завдання (наприклад, цілі, вимоги безпеки, тощо), та динамічно розподіляються залежно від їх завантаження або важливості для бізнесу. Абонентами даного сервісу є корпоративні офіси і підрозділи, ділові партнери та інші організації, які мають спільні для

використання ресурси. Інформація приватної хмари не виходить за межі корпоративної інформаційної мережі, внаслідок чого забезпечується набагато більш високий рівень захисту. Власником такого типу хмарного сервісу може являтись як сама організація, так і третя сторона або їх комбінація за певною визначеною угодою, яка встановлює розподал обов'язків з управління та обслуговування, а також забезпечення належного рівня безпеки. Фізичне розташвання ресурсів може бути як на території підприємств, так і за їхніми межами.

3) Публічна хмара (Public cloud) - хмарна інфраструктура передбачена для відкритого використання широкою публікою. Вона може перебувати у власності, управлінні і обслуговуванні ділових, наукових і урядових організацій в будь-яких їх комбінаціях. Фізичне розташвання ресурсів передбачене на території провайдера.
4) Гібридна хмара (Hybrid cloud) – даний тип розгортання хмарного сервісу являється композицією з двох або більше різних вищенаведенех моделей розгортання хмарних сервісів (приватних, публічних або громадських), що мають унікальні об'єкти, але пов'язані між собою стандартизованими або власними технологіями, які дозволяють переносити дані або застосунки між компонентами (наприклад, для балансування навантаження між хмарами).

Усі вищенаведені чотири моделі розгортання хмарних сервісів є можуть надавати сервіси трьох основних типів можливостей хмарних послуг (SPI).

Розподіл відповідальності між споживачем та хмарним провайдером

Нижченаведена таблиця (Таблиця 1.2) відображає розподіл відповідальності за управління послугами та забезпечення належного рівня безпеки послуг для моделі SPI, а також у порівнянні з розташованими на виробничому майданчику підприємства ресурсами (On – premises resources). Очевидно, що у останньому

випадку користувач є також і власником ресурсів, тому і відповідальність за фізичну безпеку, безпеку даних, віртуалізацію, розподілення ресурсів та всі інші необхідні аспекти лежить на самому підприємстві. Таким чином, в Таблиці 1.2 К – те, за що відповідає користувач, П – постачальник послуг.

Таблиця 1.2 – Розподіл відповідальності між користувачем та постачальником

Ресурси	On–premises resources	IaaS	PaaS	SaaS
Дані	К	К	К	П
Застосунки	К	К	К	П
Проміжне ПЗ	К	К	К	П
ОС	К	К	К	П
Розподіл ресурсів	К	К	П	П
Віртуалізація	К	П	П	П
Сховища даних	К	П	П	П
Мережі	К	П	П	П
Апаратне забезпечення	К	П	П	П

1.3 Архітектура хмарної інфраструктури

Архітектура хмарного сервісу складається з декількох рівнів, з них два нижніх – апаратне забезпечення та віртуалізація є фундаментальними елементами та знаходяться під повним контролем постачальника послуг, незалежно від моделі обслуговування. Модель архітектури хмарного сервісу зображено на Рисунку 1.1

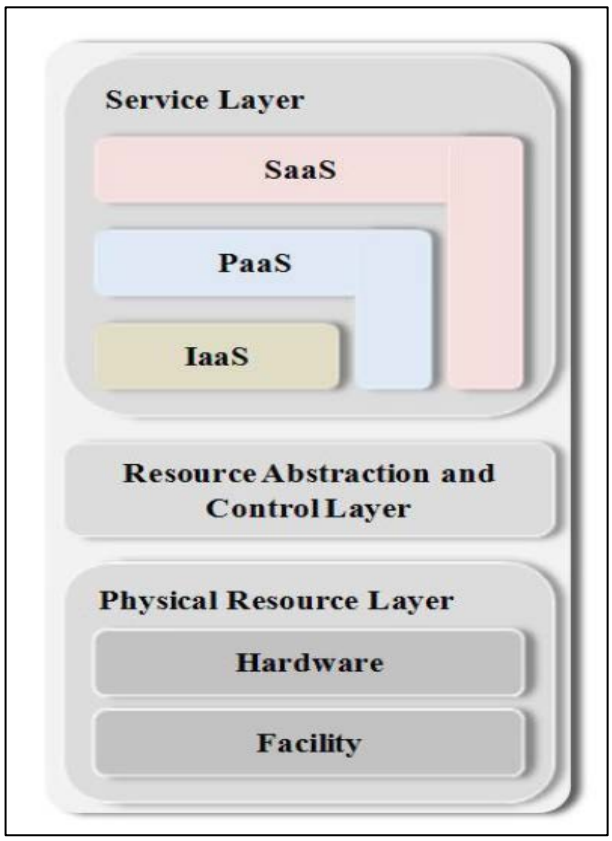

Рисунок 1.1 – Модель архітектури хмарного сервісу

Хмарні сервіси базуються на технології віртуалізації, яка передбачає абстракцію обчислюваних ресурсів або їх логічного групування. Даний підхід дозволяє групувати обчислювані ресурси від апаратної реалізації і яка забезпечує при цьому логічну ізоляцію обчислювальних процесів, що виконуються на одному фізичному ресурсі. Користувачу сервісу при цьому надаються абстракції, які не розкривають фізичної сторони обробки та зберігання даних.

Основою віртуалізації хмарного середовища є гіпервізор (або монітор віртуальних машин) – це програмний застосунок або обладнання, що забезпечує одночасне та паралельне виконання декількох операційних систем на одному і тому ж комп'ютері (хості). Гіпервізор також керує віртуальним процесором (VCPU), віртуальною пам’яттю, контролює пристрої введення/виведення та доступ до пам’яті, забезпечує ізоляцію операційних систем одну від одної, розділяє ресурси між різними запущеними ОС і керує ними, що зображено на Рисунку 1.2. Тобто гіпервізор робить можливим перехід від фізичного підходу до логічного.

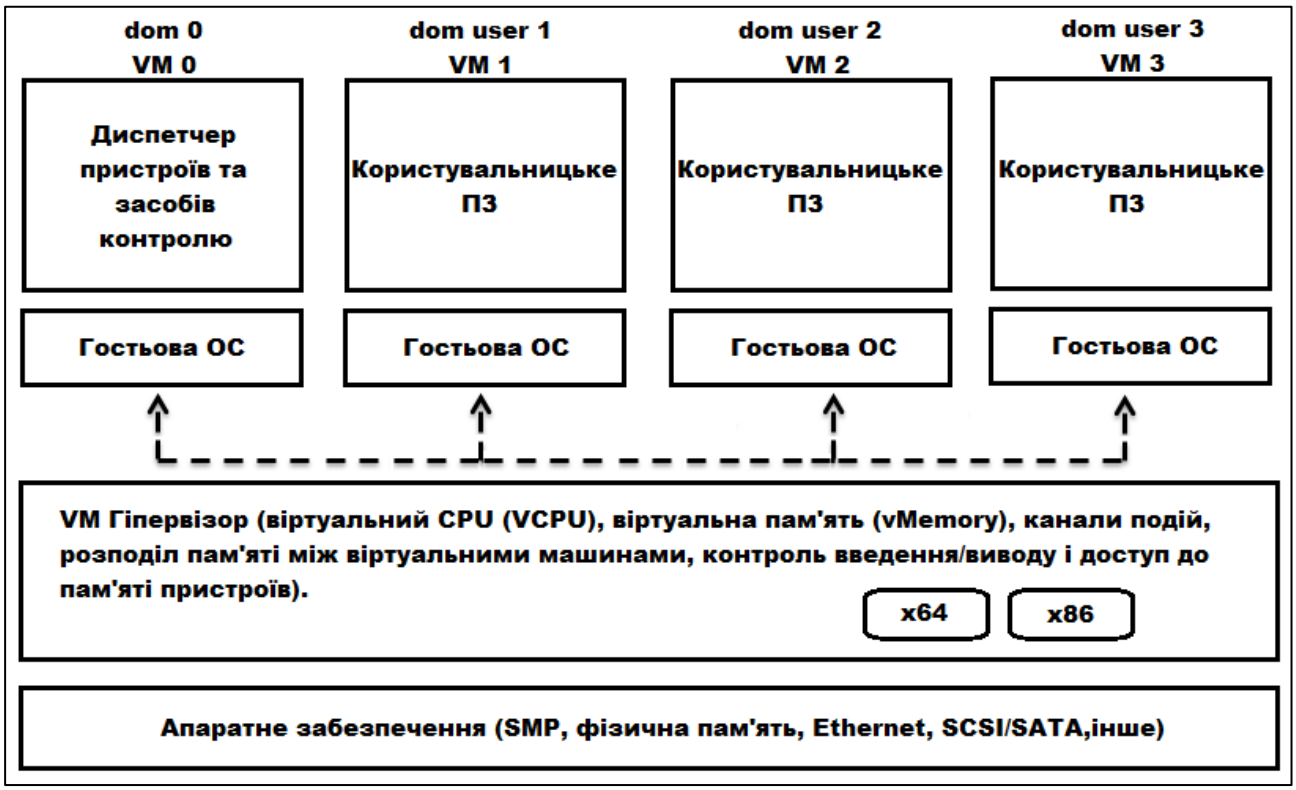

Рисунок 1.2 – Схема використання гіпервізора

Для забезпечення узгодженої роботи вузлів обчислювальної мережі на стороні хмарного провайдера використовується спеціалізоване проміжне програмне забезпечення, що забезпечує моніторинг стану обладнання і програм, балансування навантаження, забезпечення ресурсів для вирішення завдання.

Одним з найбільш вагомих рішень для згладжування нерівномірності навантаження на послуги являється розміщення шару серверної віртуалізації між шаром програмних послуг та апаратним забезпеченням. В умовах віртуалізації балансування навантаження може здійснюватися за допомогою програмного розподілу віртуальних серверів по реальним, перенесення віртуальних серверів відбувається за допомогою живої міграції.

Розглянемо деякі представлення еталонної архітектури хмарних обчислень, що пропонуються міжнародними стандартами та рекомендодавчими виданнями.

Рекомендації NIST щодо еталонної архітектури хмарних сервісів

На Рисунку 1.3 наведено огляд архітектури, Згідно з визначенням Національного інституту стандартів і технології (NIST) cloud computing, яка ідентифікує основні ролі, їх діяльність та функції в області хмарних обчислень. Діаграма зображує загальний високий рівень архітектури та призначена для полегшення розуміння вимог, їх застосування, характеристик та розуміння стандартів хмарних обчислень.

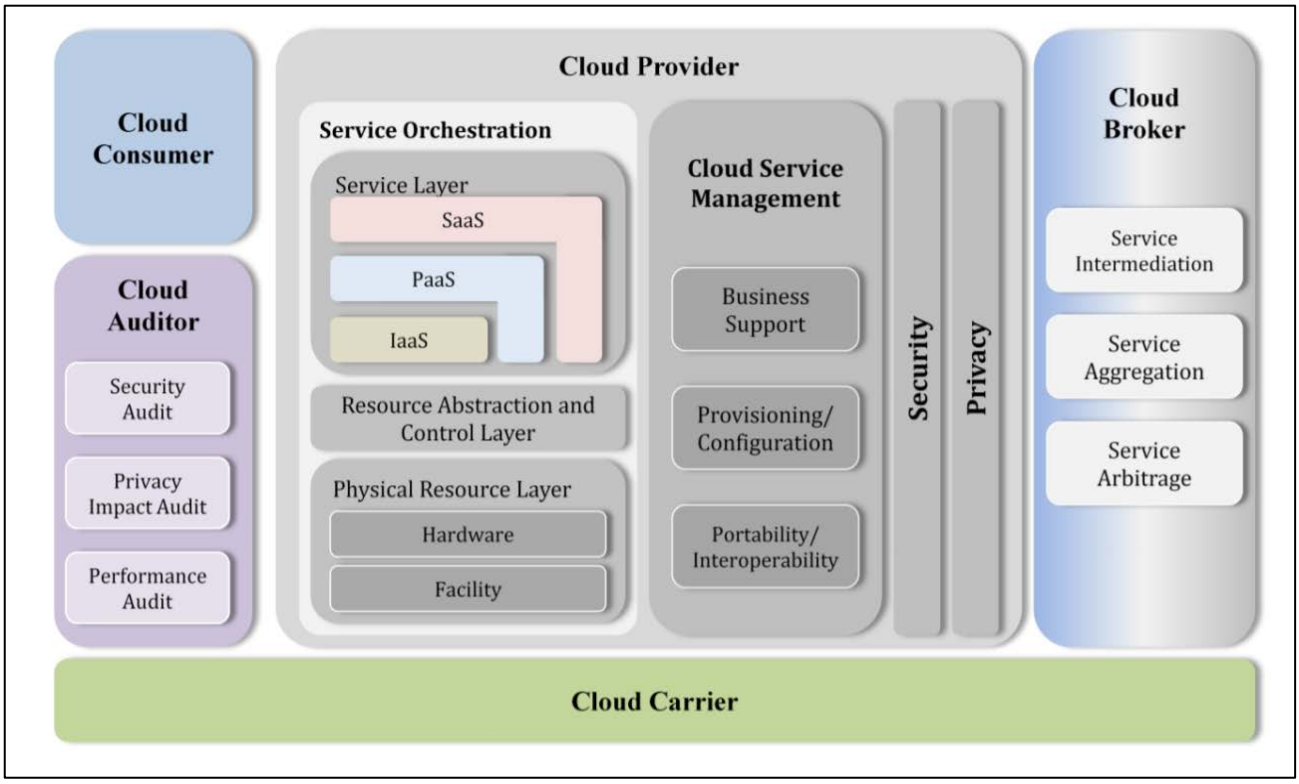

Рисунок 1.3 – Узагальнення модель хмарних сервісів

Як показано на малюнку, в NIST-довідці по архітектурі хмарних обчислень – визначено п'ять основних ролей:

- Користувач хмарного сервісу,
- Постачальник хмарного сервісу,
- оператор хмарного сервісу,
- аудитор хмарного сервісу та
- брокер.

Кожна роль- це сутність (особа або організація), яка бере участь у транзакції чи процесі та / або виконує завдання у хмарних обчислень.

В Таблиці 1.3 приведено короткий опис визначених ролей.

Таблиця 1.3 – Ролі в сфері хмарних сервісів

Ролі	**Визначення**
Користувач	Ососба або організація, яка використуває послуги хмарних сервісів, що надає постачальник.
Провайдер	Ососба, сутність чи організація, відповідальна за надання хмарних сервісів зацікавленим сторонам.
Аудитор	Сторона, яка може проводити незалежну оцінку хмарних сервісів, операцій інформаційної системи, продуктивності та безпеки реалізації хмари.
Брокер	Суб'єкт, який керує використанням, продуктивністю та доставкою хмарних сервісів та веде переговори щодо взаємовідносин між провайдером та користувачем сервісу. *Посередництво*: брокер поліпшує надану послугу, покращуючи певні можливості та надаючи додаткові послуги користувачам хмарних сервісів. Це вдосконалення може полягати в управлінні доступом до хмарних служб, управлінні ідентифікацією, звітуванні про ефективність, підвищенні безпеки тощо. *Агрегація*: брокер комбінує та інтегрує декілька сервісів в одну або кілька нових служб. Брокер забезпечує інтеграцію даних і забезпечує безпечне переміщення даних між споживачем хмарного сервісу та декількома постачальниками хмар.

Продовження таблиці 1.3

1	2
Брокер	*Арбітраж*: Сервісний арбітраж схожий на агрегування сервісу, за винятком того, що агреговані послуги не фіксуються. Сервісний арбітраж означає, що брокер має можливість вибору послуг з декількох агентств. Наприклад, брокер може скористатися послугою оцінки кредитоспроможності для вимірювання та вибору агентства з найкращим балом.
Оператор	Посередник, який забезпечує з'єднання та транспортування хмарних сервісів від постачальників до користувачів.

В нижченаведеній Таблиці 1.4 відображено можливі потоки інформації, яка є ідентифікуючими даними особи (personally identifiable information, PII) між сторонами, що беруть участь у хмарних обчисленнях, відповідно до їхніх ролей.

Таблиця 1.4 – Можливі потоки PII між визначеними ролями

№	Власник PII	Оператор	Обробник	Третя сторона
1	Постачальник PII	Постачальник PII	-	-
2	-	Постачальник PII	Постачальник PII	-
3	Постачальник PII	-	Постачальник PII	-
4	Постачальник PII	Постачальник PII	-	-
5	Постачальник PII	-	Постачальник PII	-
6	-	Постачальник PII	Постачальник PII	-
7	-	Постачальник PII	-	Постачальник PII

Продовдення таблиці 1.4

1	2	3	4	5
8	-	-	Постачальник PII	Постачальник PII

На Рисунку 1.4 ілюструється взаємодія між визначеними вище ролями. Користувач хмарного сервісу може надіслати запит безпосередньо через постачальника, або ж через брокера хмар (тобто посередника). Хмарний аудитор проводить незалежні аудити та може зв'язатися з будь-якими іншими визначеними ролями для збору необхідної інформації.

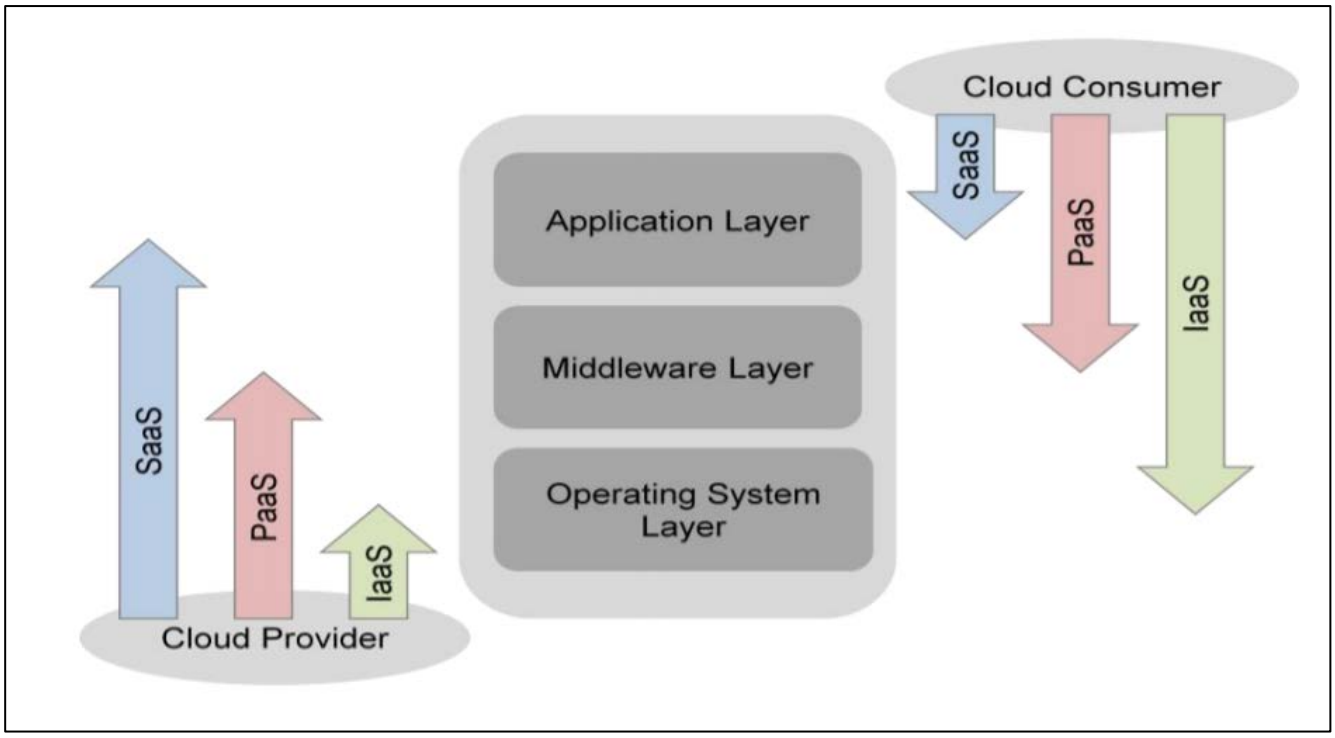

Рисунок 1.4 – Взаємодія в хмарних сервісах

- Рівень застосунків включає програмне забезпечення, призначене для кінцевих користувачів або програм. Застосункивикористовуються користувачами SaaS або встановлюються / управляються / обслуговуються споживачами PaaS, споживачами IaaS та провайдерами SaaS.

- Рівень проміжного програмного забезпечення надає програмні конструкційні блоки (наприклад, бібліотеки, бази даних та віртуальну машину Java) для розробки прикладної програми в хмарі. Проміжне програмне забезпечення використовується користувачами PaaS, встановленими / керованими / обслуговуваними споживачами IaaS або провайдерами PaaS і є прихованим від користувачів SaaS.

- Рівень ОС включає операційну систему та драйвери, та приховується від споживачів SaaS та PaaS. Хмарний сервіс IaaS дозволяє одній або декільком гостьовим операційним системам запустити віртуалізацію на одному фізичному хості. Як правило, споживачі мають широку свободу вибору, яка ОС буде розміщена з тих, що можуть бути підтримані постачальником хмарнрого сервісу. Споживачі IaaS повинні взяти на себе повну відповідальність за гостьову ОС, тоді як постачальник IaaS контролює хостинг операційної системи.

У цьому представленні використовується трирівнева модель, що представляє собою групування з трьох типів системних компонентів, які постачальники хмарних сервісів повинні забезпечувати для надання своїх послуг.

Верхній рівень моделі - це службовий рівень, саме там постачальники хмарних сервісів визначають інтерфейси користувачів для доступу до обчислювальних послуг. Доступ до інтерфейсів кожної з трьох моделей обслуговування забезпечується в цьому шарі. Можливо, але не обов'язково, що застосунки SaaS можуть бути побудовані на компонентах PaaS, а компоненти PaaS можуть бути побудовані на компонентах IaaS. Необов'язкові відносини залежностей між компонентами SaaS, PaaS та IaaS представлені графічно, оскільки компоненти сприються один на одного; тоді як калібрування компонентів означає, що кожен з сервісних компонентів може функціонувати самостійно. Наприклад, застосунок SaaS може бути реалізований і розміщений на віртуальних машинах з областей IaaS, або він може бути функціонувати безпосередньо на верхньому рівні хмарних ресурсів без використання віртуальних машин IaaS.

Середній шар у моделі - це абстракція ресурсів та шар забезпечення управління. Цей шар містить системні компоненти, які постачальники хмарних сервісів використовують для надання та керування доступом до фізичних обчислювальних ресурсів за допомогою абстракції програмного забезпечення. Приклади компонентів абстракції ресурсів включають елементи програмного забезпечення, такі як гіпервізор, віртуальні машини, віртуальні сховища даних та інші абстракції обчислювальних ресурсів. Абстракції ресурсів повинні забезпечити ефективне, безпечне та надійне використання основних фізичних ресурсів. Незважаючи на те, що технології віртуальної машини часто використовуються на цьому рівні, також можливі інші способи забезпечення необхідних абстракцій програмного забезпечення. Контрольний аспект цього рівня відноситься до програмних компонентів, які відповідають за розподіл ресурсів, контроль доступу та моніторинг використання. Він пов'язує численні основні фізичні ресурси та абстракції їх програмного забезпечення, щоб забезпечити об'єднання ресурсів, динамічне розміщення та вимірювану службу. Приклади такого типу проміжного програмного забезпечення - це різноманітні відкрите програмне забезпечення та хмарне програмне забезпечення.

Нижній рівень в стеку - це фізичний рівень ресурсів, який включає в себе всі фізичні обчислювальні ресурси. Цей рівень включає апаратні ресурси, такі як комп'ютери (процесор та пам'ять), мережі (маршрутизатори, брандмауери, комутатори, мережні посилання та інтерфейси), компоненти для зберігання (жорсткі диски) та інші елементи фізичної обчислювальної інфраструктури. Також включає в себе забезпечення фізичної безпеки ресурсів, таких як опалення, вентиляція та кондиціонування повітря (HVAC), потужність, зв'язок та інші аспекти фізичного майданчика.

Представлення еталонної архітектури хмарних сервісів згідно міжнародному стандарту ISO/IEC 17789:2014 - Information technology - Cloud computing - Reference architecture

Еталонна архітектура хмарних сервісів, представлена в цьому стандарті, являється архітектурною основою для ефективного опису ролей хмарних обчислень, підролей, діяльностей хмарних обчислень, наскрізних аспектів, а також функціональної архітектури і функціональних компонентів хмарних обчислень. Еталонна архітектура хмарних сервісів описана та може бути використана в наступних цілях:

- опис спільноти зацікавлених сторін хмарних сервісів;
- опис фундаментальних характеристик систем хмарних сервісів;
- вказівки щодо основних діяльностей хмарних сервісів і функціональних компонентів, а також опису їх відносин один з одним і з навколишнім середовищем;
- визначення принципів, які керують дизайном і еволюцією еталонної архітектури хмарних сервісів.

Еталонна архітектура хмарних сервісів підтримує наступні важливі цілі стандартизації:

- забезпечення виробництва набором узгоджених міжнародних стандартів для хмарних обчислень;
- забезпечення технологічно нейтральної контрольної точки для визначення стандартів для хмарних обчислень;
- підтримку відкритості та прозорості при ідентифікації вигод і ризиків хмарних обчислень.

У багаторівневого представлення, використовуваного в еталонній архітектурі хмарних сервісів, існують чотири рівні, а також ряд функцій, які проходять через ці рівні:

- рівень користувача;
- рівень доступу;
- рівень служби;
- рівень ресурсів.

Функції, які охоплюють ці рівні, називаються багаторівневими функціями.

Кожен з рівнів цієї структури описано нижче.

Рівень користувача

Рівень користувача - це користувацький інтерфейс, через який споживач служб хмарних обчислень взаємодіє з постачальником служб хмарних обчислень і службами хмарних обчислень, здійснює адміністративну діяльність, пов'язану зі споживачами, і здійснює моніторинг служб хмарних обчислень. Він може також передати результати хмарних обчислень для наступного рівня ресурсів.

Рівень доступу

Рівень доступу забезпечує єдиний інтерфейс для мануального та автоматизованого доступу до можливостей, доступним на рівні служб. Ці можливості включають можливості служб, а також можливості адміністрування і ділові можливості.

Рівень доступу відповідальний за представлення можливостей служб хмарних обчислень по одному (або більше) механізму доступу, наприклад, як набір веб-сторінок, до яких можна отримати доступ через браузер, або як набір веб-служб, до яких можна отримати доступ програмними засобами по захищеному каналу зв'язку. Цей рівень також відповідає за застосування відповідної функціональності безпеки для доступу до можливостей служб хмарних обчислень. Рівень доступу відповідає за аутентифікацію запиту за допомогою ідентифікуючої інформації користувача і для підтвердження авторизації користувача використовувати ті чи інші можливості. При необхідності, рівень доступу також відповідальний за обробку шифрування і перевірку цілісності запиту.

Рівень доступу може також відповідати за застосування політики якості обслуговування (QoS) до трафіку, що йде з рівня користувача (наприклад, запити до послуги для постачальника служб хмарних обчислень), і до трафіку, що йде до рівня користувача (наприклад, результати служб хмарних обчислень).

Рівень доступу передає підтверджені запити компонентам, розташованим на рівні служби. Рівень доступу приймає запити споживача служб хмарних

обчислень або запити споживання служб хмарних обчислень постачальника служб хмарних обчислень на отримання доступу до послуг і ресурсів постачальника служб хмарних обчислень.

Рівень служби

Рівень служби містить реалізацію служб, що надаються постачальником служб хмарних обчислень. Рівень служби містить і управляє компонентами програмного забезпечення, які здійснюють послуги (але не розташовані нижче гіпервізори, хостингові операційні системи, драйвери пристроїв, і т. д.) і забезпечує надання служби хмарних обчислень користувачам через рівень доступу.

Програмне забезпечення реалізації служби в рівні служби, в свою чергу, покладається на можливості, доступні в рівні ресурсу, щоб надати пропоновані послуги і гарантувати виконання вимог всіх угод про рівень послуг, що стосуються послуг, наприклад, використовуючи достатню кількість ресурсів.

Рівень ресурсів

На рівні ресурсів знаходяться ресурси, включаючи обладнання, яке зазвичай використовується в центрі обробки даних, таке як сервери, мережеві комутатори і маршрутизатори, пристрої зберігання, а також відповідне програмне забезпечення не специфічне для хмарних обчислень, яке виконується на серверах та іншому обладнанні, таке як хостингові операційні системи, гіпервізор, драйвери пристроїв і загальне програмне забезпечення, що забезпечує управління системами.

Рівень ресурсів також надає і включає в себе функціональність транспортної мережі хмари, необхідну для можливості з'єднання мережі між постачальником служб хмарних обчислень і користувачами, в рамках самого постачальника служб хмарних обчислень і між постачальниками партнерських служб хмарних обчислень.

Слід мати на увазі, що для того, щоб постачальнику служб хмарних обчислень надати послуги, сумісні з угодою про рівень послуг, можуть знадобитися виділені

і / або безпечні з'єднання між користувачами і постачальником служб хмарних обчислень.

Багаторівневі функції

Багаторівневі функції включають ряд функціональних компонентів, які взаємодіють з функціональними компонентами вищезгаданих чотирьох рівнів, щоб забезпечити допоміжні можливості, включаючи такі функції, але не обмежуючись ними:

- можливості систем оперативної підтримки (адміністрування під час виконання, моніторинг, забезпечення і супровід);
- можливості систем бізнес-підтримки (каталог продуктів, виставлення рахунків і фінансовий менеджмент);
- можливості систем безпеки (ідентифікація, дозвіл, аудит, валідація, шифрування);
- можливості інтеграції (зв'язок різних компонентів, для досягнення необхідної функціональності);
- можливості підтримки розробки (включаючи створення, управління тестуванням, управління життєвим циклом служб та компонентів служб).

Функціональний компонент - функціональний елемент еталоннної архітектури хмарних сервісів, який використовується для здійснення певної діяльності або частини діяльності, і у якого є реалізаційний артефакт в конкретній реалізації архітектури, наприклад, компонент програмного забезпечення, підсистема або застосунок.

Рисунок 1.5 є представленням високорівневого огляду функціональних компонентів еталонної архітектури хмарних сервісів, організованих в багаторівневу інфраструктуру.

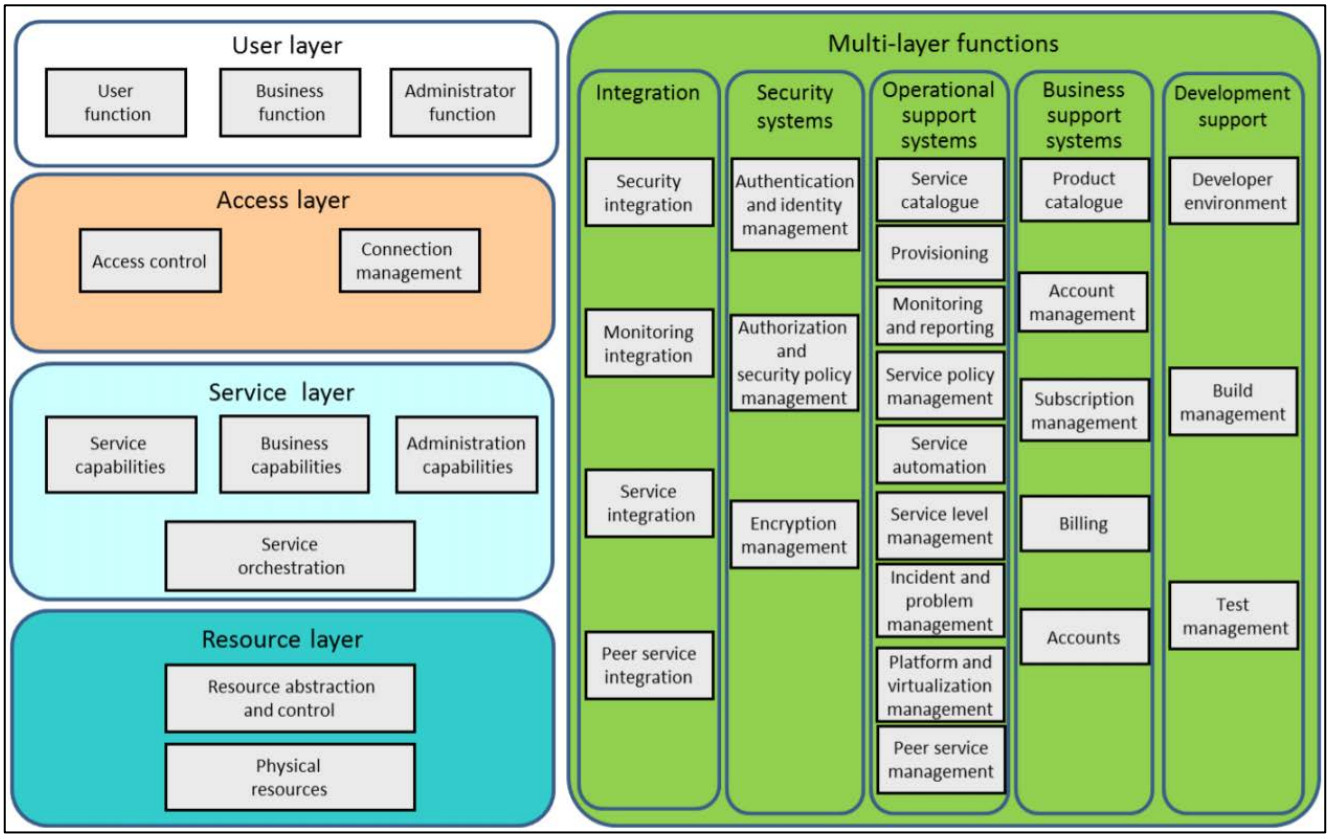

Рисунок 1.5 – Високорівневий огляд функціональних компонентів еталонної архітектури хмарних сервісів, організованих в багаторівневу інфраструктуру

1.4 База даних як сервіс

DBaaS надає СКБД як сервіс на вимогу для управління даними та здійснення необхідних операцій. Хмарна СКБД є розподіленою базою даних, яка забезпечує обчислення як сервіс, що включає спільне використання ресурсів, програмного забезпечення та інформації між багатьма пристроями через мережу Інтернет.

DBaaS може бути або частиною моделі SaaS, або PaaS – в залежності від того, яким шляхом він постачається провайдером.

Сервіс DBaaS має суттєві переваги у підтримці та супроводженні:

- надає доступ до загальної консолідованої платформи послуг бази даних через мережу Інтернет;
- забезпечує модель самообслуговування для ініціалізації потрібних споживачу ресурсів;

- забезпечує еластичне масштабування ресурсів бази даних в залежності від потреб користувача;
- забезпечує безперервну роботу з сервісами та швидке відновлення в разі падіння.

Подібний сервіс робить прозорим для користувача весь стек програмного забезпечення, що використовується для підтримки працездатності бази. Зазвичай він включає в себе операційну систему, СКБД і стороннє програмне забезпечення, що використовується безпосередньо для роботи. Постачальник послуг бере на себе відповідальність за установку, виправлення і управління даним програмним забезпеченням.

Хмарні провайдери намагаються також забезпечити усі необхідні заходи безпеки, тому разом з сервісами надають послуги:

- автентифікації та авторизації хмарних споживачів з використанням попередньо створеного мандата доступу;
- доступності: налаштування конфігурацій/призначення ресурсів для відновлення, вдосконалення і підключення нових вузлів в хмару;
- конфіденційності: виявлення та моніторинг віртуальних ресурсів, моніторинг функціонування (дій і подій) хмари і генерація звітів про продуктивність;
- управління ідентифікацією: надання можливостей кількісних вимірів на рівні абстракції, відповідному типу сервісу (наприклад, засобів зберігання, обробки, пропускної здатності та активних облікових записів користувачів);
- моніторингу безпеки та обробки інцидентів: визначення параметрів SLA (Service Level Agreement), моніторинг виконання SLA, застосування SLA відповідно до заданих політик безпеки;
- управління політиками безпеки: розробка / застосування / аудит / актуалізація політик безпеки для користувачів, які отримують доступ до хмар.

Для керування аутсорсинговими базами даних було створено модель DBaaS архітектури спеціально для хмарних обчислень. Ця модель складається з наступних рівнів:

- Рівень інтерфейсу користувача – надає доступ до хмарних сервісів через веб-браузер та Інтернет.
- Рівень застосунків – використовується для доступу до програмних сервісів та сховищ у хмарі.
- Рівень бази даних – надає ефективний та надійний сервіс управління базою даних за допомогою запитів до сховища даних.
- Рівень сховища даних – зберігає дані в зашифрованому виді та розшифровує їх за потребою, надає управління резервними копіями та здійснює моніторинг дисків.

Постачальники послуги DBaaS пропонують два види реалізації: мультиарендну архітектуру (multi-tenant) та архітектуру з чисельними екземплярами (multi-instance).

1) В мультиарендній архітектурі, зображеній на Рисунку 1.6 користувачі одночасно працюють з єдиним екземпляром СКБД, який запущений на сервері. Всі базові механізми СКБД, такі як системний каталог, каширування, оптимізатор запитів і особливості розробки додатків, будуються для підтримки додатків окремого користувача та запускаються прямо на вершині спеціально налаштованої операційної системи хосту та апаратному забезпеченні. Тож мультиарендні хмарні бази даних, побудовані зі стандартними СКБД, доступні для користування тільки за допомогою віртуалізації, яка однак негативно впливає на продуктивність СКБД за рахунок навантажень на гіпервізор. Також, головними недоліками є складність управління динамічним середовищем, в якому чисельність користувачів постійно змінюється, та підтримка ізольованої мережі для кожного користувача.

Відповідальність за підтримку і створення надійного середовища мультиарендної БД покладається виключно на постачальника хмари.

Рисунок 1.6 – Мультиарендна архітектура DBaaS

2) В архітектурі з чисельними екземплярами, зображеній на Рисунку 1.7, кожен користувач забезпечується окремим екземпляром ПЗ та СКБД, що працює на віртуальній машині, яка призначена тільки для конкретної організації-споживача послуги DBaaS. Це дозволяє користувачам мати більший контроль над адмініструванням та іншими завданнями, пов'язаними з безпекою (наприклад, визначення ролі та авторизація користувача). В цілому, ця архітектура рекомендується майже всіма постачальниками, тому що вважається більш безпечнішою за рахунок певних функцій безпеки, наприклад шифрування даних, та більш легко розгортання баз даних, ніж в мультиарендній архітектурі. Ця модель більш приваблива не тільки з точки зору безпеки, але й продуктивності, бо архітектура має чіткий поділ між клієнтськими навантаженнями.

Рисунок 1.7 – Архітектура DBaaS з чисельними екземплярами

Висновки до розділу 1

Метою даної кваліфікаційної роботи є розробка моделі системи захисту інформації для хмарної системи керування базами даних, яка дасть можливість оптимального використання ресурсів при побудові системи захисту інформації в хмарних системах керування базами даних та забезпечення належного рівня безпеки даних, що зберігаються та оброблюються в таких системах.

Методом дослідження є опрацювання літератури та інших інформаційних джерел за даною темою, розгляд міжнародних стандартів та інших документів, що регулюють галузь хмарних обчислень, аналіз існуючих методів та засобів захисту інформації та їхніх характеристик, аналіз вимог що до захисту інформації при зберіганні та обробці в хмарних системах керування базами даних.

Було проведено роботу з опрацювання літератури та інших джерел, огляд міжнародних стандартів. Встановлено класифікацію хмарних сервісів, типи можливостей надання послуг, класифікацію моделей розгортання.

2 МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ В ХМАРНИХ СКБД

2.1 Нормативно-правова документація, що врегульовує сферу захисту інформації

Стандарти часто представляють в якості рішення усіх проблем, пов'язаних з хмарними сервісами, проте ця сервісна модель базується на вже існуючих, тому досить суперечливим є питання, щодо встановлення нових стандартів, що стосуються, наприклад, надання хмарних послуг з використання застосунків. Проте можуть бути цілком корисними нові стандарти для врегулювання операційних труднощів управління хмарами, а також оціночні стандарти для визначення захищеності і надійності провайдерів.

Хмарні сервіси розглядаються різними експертами або як революційна парадигма доставки IT-сервісів, або як нова назву для способу доставки сервісів, існуючого стільки ж, скільки самі IT.

Існує певна невизначеність стосовно потреби в стандартизації сфери використання хмарних сервісів. Винятком можна вважати безпеку - в цій області спостерігається явний прогрес, що виражається, зокрема, в діяльності асоціації Cloud Security Alliance. Різниця в тому, що технічні можливості еволюціонували в такій мірі, щоб ідея, настільки давно існуюча, нарешті змогла втілитися в життя. До появи сучасних високошвидкісних каналів передачі даних централізована доставка більшості сервісів була можлива тільки з пунктів, що знаходяться від одержувача в безпосередній географічній близькості. Сучасні ж мережі дозволяють централізувати адміністрування і об'єднати продуктивність географічно розподілених серверів.

На даному етапі вийшло декілька стандартів та рекомендаційних видань, огляд яких наведено нижче:

- ISO/IEC 19944: - Дані та їх потоки між пристроями та хмарними службами. Описує різні типи даних, що надходять в хмарних обчислень, і вплив підключених пристроїв на дані, що обробляються в хмарних системах. • Розширює існуючу словниковий ресурс хмарних обчислень та базову архітектуру, щоб описати структуру, яка охоплює пристрої, що використовують хмарні сервіси. Визначає категорії даних, які надходять на пристрої клієнта хмарних сервісів, щоб допомогти користувачам хмарної служби розуміти та захищати та конфіденційність своїх даних через підвищення прозорості політики та практики.
- ISO/IEC 17788:2014 (Information technology - Cloud computing - Overview and vocabulary) – Хмарні обчислення. – Загальний огляд та словник термінів– стандарт містить визначення основних понять в сфері хмарних обчислень, у тому числі роз'яснення моделі SPI.
- ISO/IEC 17789:2014 (Information technology - Cloud computing - Reference architecture) – Хмарні обчислення. – Еталонна архітектура - в даному стандарті наведено основні принципи еталонної архітектури хмарного сервісу, описано основні ролі, які взаємодіють між собою в просторі використання хмарних технологій.
- ISO/IEC 27018:2014 (Information technology – Security techniques – Information security management systems – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors) - Інформаційні технології - Технології безпеки - Системи управління інформаційною безпекою - Кодекс практики захисту персональної інформації (PII) у публічних хмарах, що діють як PII процесори - це звід правил, який спрямований на забезпечення захисту особистих даних у хмарі. Він заснований на стандарті інформаційної безпеки ISO 27002 та містить настанови щодо застосування засобів контролю цього стандарту, які є застосовними до персональних даних, а також надає набір додаткових засобів управління та відповідні

керівництва для виконання тих вимог щодо захисту персональних даних в публічній хмарі, які не охоплюються засобами управління стандарту ISO 27002.

- ISO/IEC 27018 (draft) – містить додаткові поради щодо впровадження відповідних контролів інформаційної безпеки на основі ISO 27002.
- Проект Закону про внесення змін до деяких законодавчих актів України щодо обробки інформації в системах хмарних обчислень, а саме до наступних законів:
  - "Про захист інформації в інформаційно-телекомунікаційних системах"
  - "Про захист персональних даних".

Зміни, що пропонуються до внесення даним проектом конкретизують, що пункти статей вищенаведених законів стосуються також і сфери хмарних технологій, а також конкретизують положення про закріплення відповідальності між постачальниками послуг та споживачами на основі підписання NDA, SLA та інших додаткових договорів про надання послуг, які надалі регламентуватимуть розподіл відповідальності за рівень надання послуг та забезпечення належного рівня безпеки користувацьких даних.

2.2 Аналіз інформаційної безпеки

Захист даних передбачає новий ракурс в хмарних обчисленнях. Організація може прийняти рішення зберігати свої дані в сервісі хмарних обчислень, але тоді повинні бути ясно узгоджено розподіл відповідальності за захист даних і за наслідки. Перший крок, що виконується користувачем сервісів хмарних обчислень, полягає в тому, щоб належним чином класифікувати дані і визначити їх значимість для бізнесу і ризик в разі їх витоку, втрати або пошкодження. Як

визначити значимість даних описано в міжнародному стандарті ISO/IEC 27002:2014.

В ідеальному випадку захист даних перед завантаженням в систему хмарних обчислень повинен бути обов'язком споживача служб хмарних обчислень. Однак постачальник повинен нести відповідальність за будь-яке спотворення даних або їх крадіжку. Як заходи протидії може бути використано: шифрування, але в цьому випадку необхідно розглядати управління ключами, де споживач служб хмарних обчислень або будь-яка третя особа керують ключами. Якщо ключами управляє постачальник служб хмарних обчислень, тоді він відповідальний за логічний і фізичний контроль ключів, а також даних.

2.2.1 Загрози

Оскільки у випадку використання хмарних сервісів для зберігання та обробки даних основну цінність становить сама інформація, то, відповідно і загрози поділяються на три типи: загрози конфіденційності, цілісності та доступності даних.

Основні загрози, зстосовні до хмарних сервісів, на які неодноразово було вказано в звітах організацій та статистиках, що відображають узгоджену думку експертів щодо найбільш значних загроз безпеки в хмарних сервісах і приділяють основну увагу загрозам, що виникають зі спільного використання загальних хмарних ресурсів і звернення до них безлічі користувачів на вимогу.

Крадіжка даних

Крадіжка конфіденційної корпоративної інформації - завжди несе критичні наслідки для організації, але хмарна модель відкриває нові, значні магістралі атак. Якщо база даних хмари з множинною орендою не продумана належним чином, то вразливості в застосунках одного клієнта можуть відкрити хакерам доступ до даних не тільки цього клієнта, а й усіх інших користувачів хмархмарного сервісу.

У будь-якого хмарного сервісу є кілька рівнів захисту, кожен з яких захищає інформацію від різного типу атак. Так, наприклад, фізичний захист сервера. Тут мова йде навіть не про злом, а про крадіжки або псування носіїв інформації. Винести сервер з приміщення може бути важко в прямому сенсі цього слова. Крім цього, компанія провайдера, швидше за все, зберігає інформацію в дата-центрах з охороною, відеоспостереженням та обмеженням доступу не тільки стороннім, але і більшості співробітників компанії. Так що ймовірність того, що зловмисник просто прийде і забере інформацію, близькою до нуля.

SaaS провайдери компанії не тримають всю інформацію на одному сервері. Таким чином, злом, навіть якщо він відбудеться, стає куди менш критичним для бізнему.

Другий рівень захисту в хмарних сервісах - це захист в процесі передачі даних. SaaS-провайдери шифрують весь трафік за допомогою https-протоколу з використанням SSL-сертифіката. Так дані будуть у безпеці від спроб аналізаторів трафіку перехопити їх.

Втрата даних

Якщо постачальник хмарних послуг не забезпечить належних заходів резервного копіювання, дані випадково може видалити сам провайдер або вони постраждають під час пожежі або стихійного лиха.

Дане побоювання цілком обґрунтовано, але проблем можна уникнути шляхом впровадження процесу резервного копіювання. Компанії, які піклуються про клієнтів і про репутацію, щодня і не менше двох разів автоматично копіюють базу даних. Таким чином, якщо користувач звернувся в технічну підтримку з повідомленням про випадково видалені, але важливі файлах, їх також можна буде відновити. Така проблема також повинна вирішуватися превентивно, з боку користувача, і відноситься до питання інструктажу і комп'ютерної грамотності співробітників, а також обмеженням прав доступу до зміни і видалення файлів

Крадіжка акаунтів

У хмарному середовищі зломщик може використовувати вкрадену автентифікаційну інформацію, щоб перехоплювати, підробляти або видавати спотворені дані, перенаправляти користувачів на шкідливі сайти. Організаціям слід заборонити роздачу своїх автентифікаційних даних іншим службовцям та використання одних і тих же паролів для всіх сервісів. Потрібно також запровадити надійну, двофакторну аутентифікацію для зниження ризику.

Незахищені інтерфейси і API

Слабко захищені інтерфейси програмного забезпечення або Application Programming Interface (API), які використовуються замовниками для управління і взаємодії з хмарними послугами, піддають організацію цілому ряду загроз. Ці інтерфейси повинні бути правильно спроектовані і обов'язково включати аутентифікацію, управління доступом і шифрування, щоб забезпечити необхідний захист хмарних послуг.

Організації і сторонні підрядники часто використовують хмарні інтерфейси для надання додаткових послуг, що робить їх більш складними і збільшує ризик, оскільки може знадобитися, щоб замовник повідомив свої автентифікаційні дані такому підряднику для спрощення надання послуг.

DDoS-атаки

На хмарний сервіс можуть бути зроблені атаки типу «відмова в обслуговуванні», які викликають перевантаження інфраструктури, змушуючи задіяти величезний обсяг системних ресурсів і не даючи можливості користувачам користуватися цією послугою. Найчастіше зустрічаються випадки проведення розподілених, або DDoS-атак, але є й інші типи DoS-атак, які можуть блокувати надання провайдером хмарного сервісу відповідних послуг користувачам. Наприклад, зловмисники можуть запустити асиметричні DoS-атаки прикладного рівня, використовуючи вразливості в Web-серверах, базах даних або інших хмарних ресурсах, щоб унеможливити нормальне функціонування застосунку з дуже малим корисним навантаженням.

Зловмисний інсайдер

У середовищі IaaS, PaaS або SaaS, де не забезпечено належний рівень безпеки, інсайдер, який має непорядні наміри (наприклад, системний адміністратор), може отримати доступ до конфіденційної інформації, яка йому не призначена.

Системи, які в забезпеченні безпеки покладаються лише на постачальника хмарних послуг, піддають себе великому ризику. Навіть якщо впроваджено шифрування, то система все ще схильна до зловмисних дій інсайдера.

Атаки хакерів

Хмарні обчислення дають можливість організаціям будь-якого розміру задіяти величезну обчислювальну потужність, але хтось може захотіти зробити це з непорядними намірами. Наприклад, хакер може використовувати сукупну потужність серверів хмарного сервісу, щоб зламати шифрувальний ключ в лічені хвилини.

Постачальники хмарних послуг повинні продумати, як вони будуть відстежувати людей, що використовують потужності хмарної інфраструктури на шкоду, яким чином будуть виявлятися і запобігати такі зловживання.

Недостатня передбачливість

У гонитві за зниженням витрат і іншими перевагами хмарних сервісів деякі організації поспішають використовувати хмарні послуги, не розуміючи до кінця все наслідки цього кроку. Організації повинні провести велику, ретельну перевірку своїх внутрішніх систем і потенційного постачальника хмари, щоб повністю усвідомити всі ризики, яким вони себе піддають, переходячи на нову модель.

Суміжна вразливість

У будь-якої моделі хмарної доставки існує загроза уразливості через загальні ресурси. Якщо ключовий компонент спільно використовуваної технології - наприклад, гіпервізор або елемент загальної платформи - буде зламаний, то це

піддає ризику не тільки потерпілого користувача: вразливою стає все середовище хмарного сервісу.

Хмарні сервіси можуть працювати повільно

Досить популярна претензія до хмарних сервісів. Дійсно, робота таких сервісів може бути нестабільною, що зумовлено віддаленістю та розподіленістю ресурсів та через проблеми з інтернет з’єднанням. Повільно, але вірно ситуація по даному питанню налагоджується.

2.2.2 Атаки на хмарні сервіси та рішення щодо їх усунення

Традиційні атаки на ПЗ

Вразливості операційних систем, модульних компонентів, мережевих протоколів - традиційні загрози, для захисту від яких досить встановити міжмережевий екран, firewall, антивірус, сістеме запобігання вторгнень (Intrusion Prevention System - IPS) і інші компоненти. При цьому важливо, щоб ці засоби захисту ефективно працювали в умовах віртуалізації.

Функціональні атаки на елементи хмари

Цей тип атак пов'язаний з багатошаровістю хмари, загальним принципом безпеки. Для захисту від функціональних атак для кожної частини хмарного сервісу необхідно використовувати такі засоби захисту: для проксі - ефективний захист від DoSатак, для веб-сервера - контроль цілісності сторінок, для сервера додатків - екран рівня додатків, для СКБД - захист від SQL-ін'єкцій, для системи зберігання даних - правильні бекапи (резервне копіювання), розмежування доступу. Окремо кожні з цих захисних механізмів вже створені, але вони не зібрані разом для комплексного захисту хмари, тому завдання по інтеграції їх в єдину систему потрібно вирішувати під час створення хмарного сервісу.

Атаки на клієнта

Більшість користувачів підключаються до хмари, використовуючи браузер. Тут розглядаються такі атаки як Cross Site Scripting, «викрадення» паролів, перехоплення веб-сесій, «man-in-the-middle» і багато інших. На поточний момент, найбільш ефективним захистом від даного виду атак є правильна аутентифікація і використання шифрованого з'єднання (SSL) з взаємною аутентифікацією. Однак ці кошти захисту не дуже зручні і дуже марнотратні для творців хмар. У цій галузі інформаційної безпеки є ще безліч невирішених завдань.

Атаки на гіпервізор

Гіпервізор є одним з ключових елементів віртуальної системи. Основною його функцією є поділ ресурсів між віртуальними машинами. Атака на гіпервізор може привести до того, що одна віртуальна машина зможе отримати доступ до пам'яті і ресурсів іншої. Також вона зможе перехоплювати мережевий трафік, відбирати фізичні ресурси і навіть витіснити віртуальну машину з сервера. В якості стандартних методів захисту рекомендується застосовувати спеціалізовані продукти для віртуальних середовищ, інтеграцію хост-серверів зі службою каталогу Active Directory, використання політик складності і старіння паролів, а також стандартизацію процедур доступу до керуючих засобів хост-сервера, вбудований брандмауер хоста віртуалізації. Також можливе відключення таких часто невикористовуваних служб як, наприклад, веб-доступ до сервера віртуалізації.

Атаки на системи управління

Велика кількість віртуальних машин, які використовуються в хмарах, вимагає наявності систем управління, здатних надійно контролювати створення, перенесення та утилізацію віртуальних машин. Втручання в систему управління може привести до появи віртуальних машин, здатних блокувати одні віртуальні машини і підставляти інші.

2.2.3 Рішення з захисту від загроз інформаційної безпеки

1. **Шифрування**

Шифрування - один з найефективніших способів захисту даних. Провайдер, що надає доступ до даних, повинен шифрувати інформацію клієнта, що зберігається в ЦОД, а також, в разі відсутності необхідності, безповоротно видаляти.

2. **Захист даних при передачі**

Зашифровані дані при передачі повинні бути доступні тільки після аутентифікації. Дані не вийде прочитати або зробити зміни, навіть в разі доступу через ненадійні вузли. Такі технології досить відомі, алгоритми і надійні протоколи AES, TLS давно використовуються провайдерами.

3. **Аутентификация**

Автентифікація - захист паролем. Для забезпечення більш високої надійності часто вдаються до таких засобів як токени і сертифікати. Для прозорої взаємодії провайдера з системою ідентифікації при авторизації також рекомендується використовувати LDAP (Lightweight Directory Access Protocol) і SAML (Security Assertion Markup Language).

4. **Ізоляція користувачів**

Використання індивідуальної віртуальної машини і віртуальної мережі. Віртуальні мережі повинні бути розгорнуті із застосуванням таких технологій як VPN (Virtual Private Network), VLAN (Virtual Local Area Network) і VPLS (Virtual Private LAN Service). Часто провайдери ізолюють інформацію користувачів один від одного за рахунок зміни коду в єдиному програмному середовищі. Такий підхід має ризики, пов'язані з небезпекою знайти недоліки в нестандартному коді і отримати доступ до даних користувачів. У разі можливої помилки в коді один користувач може отримати дані іншого користувача.

2.3 Структура моделі системи захисту інформації

2.3.1 Захист каналів зв’язку

Доступ до хмарного сервісу може здійснюватись через веб-браузер з використанням захищеного протоколу передачі даних HTTPS (HTTP over SSL / TLS). При використанні HTTPS в URL буде відображено, що передача даних відбувається по протоколу HTTP , але використовується інший порт за замовчуванням – 443, а також додатковий шар шифрування між HTTP і TCP. Дана схема забезпечує виконання захисту автентифікації, а також шифрування комунікацій і повсюдно використовується для передачі даних через мережу, коли забезпечення безпеки комунікацій є важливим аспектом, наприклад, при передачі даних у платіжних системах, тощо.

При передачі даних з використанням HTTPS відбувається шифрування переважної більшості його основних елементів, оскільки в цьому випаду HTTP передається через протоколи SSL або TLS, наприклад - URL-запити, включаючи шлях та назву ресурсу (сторінки), параметри запиту, заголовки та куки, які часто містять ідентифікаційні дані користувача. При цьому і даному випадку шифруванню не підлягають: назва або адреса хоста (веб-сайту) та порт, оскільки вони використовуються транспортним протоколом TCP/IP для встановлення з'єднання. Шифрування гарантує певний ступінь захисту від прослуховування та від атаки «людина посередині» (man-in-the-middle), за умови, якщо конфігурації протоколу є коректними, а сертифікат підписано авторизованим центром сертифікації. TCP портом за замовчуванням для HTTPS є 443, для HTTP — 80.

Щоб підготувати веб-сервер для прийняття https-транзакцій, адміністратору необхідно створити сертифікат з відкритим ключем для веб-сервера. Створення таких сертифікатів можливо за допомогою спеціального ПЗ, встановленого UNIX сервері, такого як OpenSSL. Необхідним є підписання даного сертифікату уповноваженим органом сертифікації (certificate authority), який засвідчує

однозначну ідентифікацію сертифікату з отримувачем. Браузери розповсюджуються з сертифікатами центрів сертифікації верхнього рівня, що дозволяє браузерові перевіряти сертифікати, які були підписані даними центрами.

Довіряти HTTPS з'єднанню можна тоді і тільки тоді, коли всі нижченаведені твердження є коректними:

Користувач довіряє тому, що у браузері правильно забезпечено підтримку HTTPS із коректними попередньо встановленими сертифікатами уповноважених на видачу сертифікатів.

- Користувач довіряє тому, що уповноважені на видачу сертифікатів засвідчують тільки відповідні (справжні) веб-сайти.
- Веб-сайт надає дійсний сертифікат, тобто підписаний довіреним центром сертифікації.
- Сертифікат конкретно розпізнає веб-сайт (тобто коли браузер відвідує сторінку "https://example.com", отриманий сертифікат правильний для "example.com", а не для інших доменних імен).
- Користувач довіряє тому, що криптографічний рівень (шифрування за допомогою SSL/TLS) достатньо надійний, щоб захиститися від дешифрування.
- Протокол HTTPS особливо важливий у незахищених мережах (таких як публічні Wi-Fi точки доступу), оскільки будь-хто в локальних мережах може аналізувати трафік та перехоплювати чи змінювати інформацію, не захищену HTTPS. Це означає, що гіпотетичний зловмисник може потенційно красти приватні дані користувача, отримувати доступ до облікового запису, вставляти шкідливий програмний код чи посилання на програмне забезпечення у сторінки, що надсилаються користувачеві у відповідь на його запити, тощо.

Організації можуть також мати власних уповноважених на видачу сертифікатів, особливо якщо вони відповідальні за конфігурацію браузерів, що мають доступ до їх власних сайтів (наприклад, сайти внутрішньої мережі

компанії), оскільки вони можуть тривіально додати свій власний сертифікат до браузера.

Деякі сайти використовують самостійно підписані сертифікати. Їх використання забезпечує захист проти підслуховування, але є ризик нападу «людина-посередині». Для запобігання нападу необхідна перевірка сертифікату іншим методом (наприклад подзвонити власнику сертифіката задля перевірки контрольної суми сертифіката).

Система може також використовуватися для клієнтської автентифікації, щоб обмежити доступ до веб-сервера тільки зареєстрованими користувачами. Для цього адміністратор сайту створює сертифікати для кожного користувача, які завантажуються в їхні браузер. Такі сертифікати зазвичай містять ім'я і електронну пошту зареєстрованого користувача, й автоматично перевіряються сервером при кожному повторному підключенні. Повторне введення паролю не потрібне.

Протокол SSL

Протокол SSL складається з двох підпротоколів: протокол SSL запису і рукостискання. Протокол SSL запису визначає формат, який використовується для передачі даних. Протокол SSL включає рукостискання з використанням протоколу SSL запису для обміну серіями повідомлень між сервером і клієнтом, під час встановлення першого з'єднання. Для роботи SSL потрібно, щоб на сервері був SSL-сертифікат.

SSL надає канал, що має три основні властивості:

- Автентифікація. Сервер завжди автентифікований, в той час як клієнт автентифікований в залежності від алгоритму.
- Цілісність. Обмін повідомленнями включає в себе перевірку цілісності.
- Конфіденційність каналу. Шифрування використовується після встановлення з'єднання і використовується для всіх наступних повідомлень.

Алгоритми, что використовують в SSL:

- Для обміну ключами та перевіркі їх достовірності застосовуються: RSA, Diffie-Hellman, ECDH, SRP, PSK.

- Для аутентіфікації: RSA, DSA, ECDSA.
- Для симетричного шифрування: RC4, IDEA, Triple DES або AES, Camellia.
- Для хеш-функцій: SHA1, SHA2, MD5.

Протокол SSH

Secure Shell, SSH— мережевий протокол рівня застосунків, що дозволяє проводити віддалене управління комп'ютером і тунелювання TCP-з'єднань (наприклад, для передачі файлів). Даний протокол шифрує весь трафік, в тому числі і паролі, що передаються.

Криптографічний захист протоколу SSH не фіксований, можливий вибір різних алгоритмів шифрування. Клієнти і сервери, що підтримують цей протокол, доступні для різних платформ. Крім того, протокол дозволяє не тільки використовувати безпечний віддалений shell на машині, але і туннелювати графічний інтерфейс. Так само ssh здатний передавати через безпечний канал (Port Forwarding) будь-який інший мережевий протокол, забезпечуючи (при належній конфігурації) можливість безпечної передачі даних.

Підтримка SSH реалізована у всіх UNIX системах, і на більшості з них в числі стандартних утиліт присутні клієнт і сервер ssh. Існує безліч реалізацій SSH-клієнтів і для не-UNIX ОС. Велику популярність протокол отримав після широкого розвитку сніферів, як альтернативне небезпечному телнету рішення для управління важливими вузлами.

Зараз відомо дві гілки версій — 1 і 2. Проте гілка 1 зупинена, оскільки було знайдено багато вразливостей, деякі з яких досі накладають серйозні обмеження на її використання, тому перспективною (такою, що розвивається) і найбезпечнішою є версія 2.

Рекомендації щодо використання крипто-наборів

Перевірити наскільки обрані набори криптографії є надійними та актуальними можна за допомогою безкоштовного сервісу ssllabs.com.

Нижче наведені рекомендації стосовно використання крипто-наборів у Таблиці 2.1.

Таблиця 2.1 – Сценарії використання криптонаборів

Сценарій	Опис
1	2
Розширений + / Advanced+ (A+)	Обмежена сумісність, наприклад до найновіших версій браузера; • Необхідність перевірки сумісності перед використанням; • Включає в себе виключно найсильніші шифри perfect forward secrecy (PFS); • Протоколи: TLS 1.2
Розширений + / Advanced+ (A+)	Ширша сумісність, наприклад для більшості нових версій браузера; • Необхідність перевірки сумісності перед використанням; • Включає в себе найсильніші / сильні шифри perfect forward secrecy (PFS); • Протоколи: TLS 1.2
Широка сумісність / Broad Compatibility (B)	Широка сумісність із веб-браузерами, необхідна перевірка сумісності з іншими протоколами перед використанням, наприклад, IMAPS • Необхідність перевірки сумісності перед використанням; • Включає в себе шифри perfect forward secrecy (PFS); • Можливість появи додаткових ризиків та нових вразливостей при використанні; • Протоколи: TLS 1.2, TLS 1.1, TLS 1

Продовження таблиці 2.1

1	2
Найширша сумісність / Widest Compatibility (C)	Сумісність із більшістю старих веб-браузерів, застарілих бібліотек (які все ще підтримуються) та інших протоколів застосунків, окрім https, наприклад IMAPS • Допустимо для використання при можливості контролю серверу, з використанням при цьому клієнтами застарілих версій браузерів та старих бібліотеки, або при використанні інших протоколів, відмінних від https; • Можливість появи додаткових ризиків та нових вразливостей при використанні є більшою, на відміну від попередніх варіантів; • Пріоритетними є шифри PFS, крім усіх шифрів DHE, які використовують SHA-1 (для запобігання можливих проблем несумісності, пов’язаних з довжиною DH); • Необхідне планування переходу до "A" для https або принаймні "B", інакше є ризик застарівання в середньостроковій перспективі; • Протоколи: TLS 1.2, TLS 1.1, TLS 1
Застарілі / Legacy (C-)	Найширша сумісність з відносно найстарішими версіями браузерів та застарілими бібліотеками та іншими протоколами застосунків, такими як SMTP • Допускається використання тільки якщо виникає ситуація вимушеного використання 3DES для застарілих клієнтських браузерів та

Продовження таблиці 2.1

1	2
	бібліотек, або при використанні інших протоколів, відмінних від https; • Необхідно враховувати можливість появи додаткових ризиків та нових вразливостей при використанні є більшою, на відміну від попередніх варіантів; • В жодному разі не рекомендується використання застарілих шифрів на основі RC2, RC4, DES, MD4, MD5, EXP, EXP1024, AH, ADH, aNULL, eNULL, SEED та IDEA; • Пріоритетними є шифри PFS, крім усіх шифрів DHE, які використовують SHA-1 (для запобігання можливих проблем несумісності, пов'язаних з довжиною DH); • Необхідне планування переходу до "C" в короткостроковій перспективі; Протоколи: TLS 1.2, TLS 1.1, TLS 1

Таблиця 2.2 – Рекомендовані до використання критпо-набори за їх пріоритизації («1» - найвищий пріоритет до використання відповідно)

Криптонабори та їх пріоритизація до використання	**Advanced+ (A+)**	**Advanced (A)**	**Broad Compatibility (B)**	**Widest Compatibility (C)**	**Legacy (C-)**
1	2	3	4	5	6
TLS_DHE_RSA_WITH_ AES_256_GCM_SHA384, [DHE-RSA-AES256-GCM-SHA384]	1	1	1	1	1

Продовження таблиці 2.2

1	2	3	4	5	6
TLS_DHE_RSA_ WITH_AES_128_GCM_SHA256, [DHE-RSA-AES128-GCM-SHA256]	2	2	2	2	2
TLS_ECDHE_RSA_WITH_ AES_256_GCM_SHA384, [ECDHE-RSA-AES256-GCM-SHA384]	3	3	3	3	3
TLS_ECDHE_RSA_WITH_ AES_128_GCM_SHA256, [ECDHE-RSA-AES128-GCM-SHA256]	4	4	4	4	4
TLS_DHE_RSA_WITH_ AES_256_CBC_SHA256, [DHE-RSA-AES256-SHA256]	-	5	5	5	5
TLS_DHE_RSA_WITH_ AES_128_CBC_SHA256, [DHE-RSA-AES128-SHA256]	-	6	6	6	6
TLS_ECDHE_RSA_WITH_ AES_256_CBC_SHA384, [ECDHE-RSA-AES256-SHA384]	-	7	7	7	7
TLS_ECDHE_RSA_WITH_ AES_128_CBC_SHA256, [ECDHE-RSA-AES128-SHA256]	-	8	8	8	8
TLS_ECDHE_RSA_WITH_ AES_256_CBC_SHA, [ECDHE-RSA-AES256-SHA]	-	-	9	9	9
TLS_ECDHE_RSA_WITH_ AES_128_CBC_SHA, [ECDHE-RSA-AES128-SHA]	-	-	10	10	10

Продовження таблиці 2.2

1	2	3	4	5	6
TLS_RSA_WITH_ AES_256_GCM_SHA384, [AES256-GCM-SHA384]	-	-	-	11	11
TLS_RSA_WITH_ AES_128_GCM_SHA256, [AES128-GCM-SHA256]	-	-	-	12	12
TLS_RSA_WITH_ AES_256_CBC_SHA256, [AES256-SHA256]	-	-	-	13	13
TLS_RSA_WITH_ AES_128_CBC_SHA256, [AES128-SHA256]	-	-	-	14	14
TLS_RSA_WITH_ AES_256_CBC_SHA, [AES256-SHA]	-	-	-	15	15
TLS_RSA_WITH_ AES_128_CBC_SHA, [AES128-SHA]	-	-	-	16	16

Слід зауважити, що не рекомундуються до використання старі версії браузерів та Java, оскільки вони не підтримують Diffie-Hellman >1024 біт. Таким чином, використання таких криптонаборів, як «TLS_DHE_RSA_WITH_AES_256_CBC_ SHA» і «TLS_DHE_RSA_WITH_AES_128_CBC_SHA» рекомендується використовувати з останнім пріоритетом для запобігання можливим випадкам несумісності, також можливо повне виключення даних двох криптонаборів зі списку.

2.3.2 Автентифікація та авторизація користувачів

Ідентифікація – процедура розпізнавання користувача в системі як правило за допомогою наперед визначеного імені (ідентифікатора) або іншої апріорної інформації про нього, яка сприймається системою.

Автентифікація – процедура встановлення належності користувачеві інформації в системі пред'явленого ним ідентифікатора.

Ідентифікація виконується, коли користувач робить спробу отримати доступ до ресурсу. Користувач повідомляє системі за її запитом свій ідентифікатор, і система перевіряє в своїй базі даних його наявність. При автентифікації користувач підтверджує свою ідентифікацію, вводячи в систему унікальну, невідому іншим користувачам інформацію про себе (наприклад, пароль або сертифікат). Ідентифікація та автентифікація є взаємопов'язаними процесами розпізнавання і перевірки дійсності користувачів, від яких залежить подальше рішення системи дозволити доступ до ресурсів системи конкретному користувачеві. Після ідентифікації і автентифікації суб'єкта виконується його авторизація, що встановлює сферу дії користувача і доступні йому ресурси.

Авторизація – процедура надання суб'єкту певних повноважень і ресурсів у даній системі.

Організація, що споживає хмарні сервіси, повинна визначити необхідний рівень безпеки на основі чітко встановлених вимог безпеки. Надійна автентифікація гарантує, що тільки авторизовані користувачі отримають доступ до контрольованої інформації.

Для захисту каналів передачі даних повинна виконуватися взаємна автентифікація суб'єктів, що зв'язуються між собою по лініях зв'язку. Процедура підтвердження автентичності виконується на початку сеансу в процесі встановлення з'єднання абонентів.

У хмарах використовується базовий принцип «єдиного входу» (Single Sign-On), який дозволяє користувачеві одноразово пройти процедуру автентифікації та отримати доступ до декількох додатків та послуги в середовищі хмарних обчислень за допомогою одного логіна, таким чином дозволяючи строгу автентифікацію на рівні користувача. Тому передбачається централізована

служба автентифікації, яка виконується одним із серверів хмари і використовує для своєї роботи базу даних . У цій базі даних зберігаються облікові дані про користувачів хмарних послуг, в яких поряд з іншою інформацією включені ідентифікатори та паролі користувачів.

Хмарні сервіси, в тому числі DBaaS, використовують стандартні методи строгої автентифікації. Відповідно до рекомендацій розрізняють процедури строгої автентифікації наступних типів:

- Одностороння автентифікація передбачає обмін інформацією тільки в одному напрямку та дозволяє: підтвердити справжність тільки однієї сторони інформаційного обміну; виявити порушення цілісності переданої інформації; гарантувати, що автентифікованими даними, які передаються по мережі, може скористатися тільки перевіряюча сторона.
- Двостороння аутентифікація в порівнянні з односторонньою містить додаткову відповідь перевіряючої сторони до генеруючої сторони, яка повинна переконувати останню, що зв’язок встановлений саме з тією стороною, для якої призначені автентифікаційні дані.
- Тристороння автентифікація містить додаткову передачу даних від генеруючої сторони до перевіряючої.

Протокол Oauth

Протокол OAuth (Open Authorization) — це відкритий стандарт авторизації, який дозволяє користувачам відкривати доступ до своїх даних, що зберігаються на одному сайті, іншому сайту, без необхідності вводу імені користувача та паролю.

Протокол OAuth дозволяє користувачам роздавати сайтам маркери доступу, до даних що розміщуються на сайтах-сервісах. Кожен маркер доступу надає доступ конкретному сайту до конкретних ресурсів та на визначений термін (короткочасний). Це дозволяє користувачам надавати доступ третім сайтам до їх інформації, що зберігається на інших сайтах — постачальниках послуг, не передаючи повною мірою самих даних та без застосування імені/паролю.

Переваги використання протоколу:

- При використанні OAuth-авторизації користувач не передає свій логін і пароль до захищених ресурсів безпосередньо.
- У користувача більше підстав довіряти застосункам, оскільки користувач може бути впевнений, що несанкціонований доступ до його особистих даних неможливий. Не володіючи логіном і паролем користувача, застосунок зможе виконувати тільки ті дії з даними, які дозволив користувач, і ніякі інші.
- При розробці програми не потрібно піклуватися про забезпечення конфіденційності логіна і пароля користувача. Логін і пароль не передаються застосунку, а отже, вони не можуть потрапити в руки зловмисників.

У разі авторизації без використання протоколу OAuth користувачеві необхідно передавати свій логін і пароль. У цього способу існують додаткові недоліки

- Якщо користувач змінює пароль, то застосунок більше не може отримати доступ до захищених ресурсів.
- Єдиний спосіб заборонити додатком доступ до захищених ресурсів - змінити пароль. Це одночасно заборонить доступ до ресурсів і іншим додаткам, які раніше його мали.
- Сервіси, що зберігають захищені ресурси, які можуть надати API для доступу до них, можуть використовувати федеративні механізми аутентифікації (англ. Federated Authentication), такі як OpenID або SAML, що дозволяє користувачам не мати пароля до їх акаунтів. Це робить неможливим для цих користувачів використання додатків, на якій знаходяться доступ до захищених ресурсів через цей API.

Версійність

На даний момент актуальною версією протоколу вважається 2.0. Окрім нових потоків в нього також було додано:

- Токен на пред’явника;

- Спрощений підпис для усунення необхідності в спеціальному аналізі, кодуваннях та сортуванні параметрів;
- Токени з которким часом існування, таким чином сервер надає токен з коротким часом існування для короткочасного доступу та довготривалу можливість оновлення токену без безпосередньої участі в цьому користувача;
- Розділення ролей – за процес авторизації та надання доступу до API можуть відповідати різрні розподілені сервери.

Двофакторна автентифікація з використанням google сервісів

Двофакторна автентифікація (ДФА, англ. two-factor authentication, також відома як двоетапна верифікація), є типом багатофакторної аутентифікації. ДФА — представляє собою технологію, що забезпечує ідентифікацію користувачів за допомогою комбінації двох різних компонентів. Хорошим прикладом двофакторної аутентифікації є авторизація Google і Microsoft. Коли користувач заходить з нового пристрою, крім аутентифікації по імені та паролю, його просять ввести шестизначний (Google) або восьмизначний (Microsoft) код підтвердження. Ви можете отримати його за допомогою SMS, або голосового дзвінка на ваш телефон, він може бути взятий з заздалегідь складеного реєстру разових кодів або ви можете використовувати додаток-аутентифікатор, генеруючий новий одноразовий пароль за короткі проміжки часу. Вибрати один з методів можна в налаштуваннях вашого Google або Microsoft-акаунта.

Переваги двофакторної автентифікації також полягають у використанні мобільних пристроїв:

- Не потрібні додаткові токени, тому що мобільний пристрій завжди під рукою.
- Код підтвердження постійно змінюється, а це безпечніше, ніж однофакторний логін-пароль

Недоліки двофакторної автентифікації через мобільний пристрій:

- Мобільний телефон повинен ловити мережу, коли відбувається аутентифікація, інакше повідомлення з паролем просто не дійде.

- Ви ділитеся з кимось вашим мобільним телефоном, що впливає на ваше особисте життя і може бути в майбутньому на нього буде приходити спам.
- Текстові повідомлення (SMS), які, потрапляючи на ваш мобільний телефон, можуть бути перехоплені.
- Текстові повідомлення приходять з деякою затримкою, так як деякий час йде на перевірку.
- Сучасні смартфони використовуються як для одержання пошти, так і для отримання SMS. Як правило електронна пошта на мобільному телефоні завжди включена. Таким чином, усі акаунти, для яких пошта є ключем, можуть бути зламані (перший фактор). Мобільний пристрій (другий фактор). Висновок: смартфон має обидві характеристики.

Зараз майже всі великі сервіси, такі як Microsoft, Google, Yandex, Dropbox, Facebook, вже надають можливість використовувати двофакторну аутентифікацію. Причому для всіх з них можна використовувати єдиний додаток аутентифікатор, що відповідає певним стандартам, такі як Google Authenticator, Microsoft Authentificator, Authy або FreeOTP.

Строга автентифікація, що базується на симетричних алгоритмах

Для роботи протоколів автентифікації, побудованих на основі симетричних алгоритмів, необхідно, щоб перевіряюча і генеруюча сторони з самого початку мали один і той же секретний ключ. Для цього часто використовуються протоколи автентифікації за участю довіреної сервера, з яким кожна сторона поділяє знання секрету. Такий сервер розподіляє сеансові ключі для кожної пари користувачів кожен раз, коли один з них запитує автентифікацію іншого.

1. **Протоколи автентифікації з симетричними алгоритмами шифрування**

Ці протоколи визначені в стандарті та пропонують попередній розподіл секретних ключів. Варіанти такої автентифікації:

- одностороння автентифікація з використанням міток часу
- одностороння автентифікація з використанням випадкових чисел
- двостороння автентифікація з використанням випадкових чисел

У кожному з цих випадків користувач доводить свою справжність, демонструючи знання секретного ключа, так як робить дешифрування запитів за допомогою цього секретного ключа.

Введемо наступні позначення:

- r_A – випадкове число, згенероване учасником A
- r_B – випадкове число, згенероване учасником B
- t_A – мітка часу, згенерована учасником A
- E_K – симетричне шифрування з ключем K, що попередньо розподілений між учасниками A та B.

1) одностороння автентифікація з використанням міток часу:

   $A \to B: E_K(t_A, B)$

   Після отримання та розшифрування цього повідомлення учасник B переконується в тому, що мітка часу t_A дійсна та ідентифікатор B співпадає з його власним. Запобігання повторної передачі даного повідомлення грунтується на тому, що без знання ключа неможливо змінити мітку часу t_A і ідентифікатор B.

2) одностороння автентифікація з використанням випадкових чисел

   $A \leftarrow B: r_B$

   $A \to B: E_K(r_B, B)$

   Учасник B відправляє учаснику A випадкове число r_B. Учасник A шифрує повідомлення, що складається з отриманого числа r_B та ідентифікатора B, та відправляє зашифроване повідомлення учаснику B. B розшифровує повідомлення і порівнює випадкове число з тим, яке відправив учаснику A, та додатково перевіряє ім’я, вказане в повідомлені.

3) двостороння автентифікація, що використовує випадкові значення

   $A \leftarrow B: r_B$

   $A \to B: E_K(r_A, r_B, B)$

   $A \leftarrow B: E_K(r_A, r_B)$

При отриманні другого повідомлення B виконує ті ж перевірки, що зазначені в попередньому протоколі, і додатково розшифровує випадкове число r_A для включення його у третє повідомлення для учасника A. Третє повідомлення дозволяє A переконатися на основі перевірки значень r_A та r_B, що він встановив канал зв'язку саме з учасником B. Прикладами такого виду автентифікації є протокол розподілу секретних ключів Нідхема і Шредера і протокол Kerberos.

2. Протоколи, засновані на використанні односпрямований ключових хеш-функцій

Протоколи, представлені вище, можуть бути модифіковані шляхом заміни симетричного шифрування на шифрування за допомогою односторонньої ключовий хеш-функції. Це буває необхідно, якщо алгоритми блокового шифрування недоступні або не відповідають пропонованим вимогам.

Одностороння хеш-функція h_KM з параметром-ключем K шифрує дані M та в результаты видає хеш-значення m (дайджест), який складається з фіксованого числа байтів. Дайджест $m = h_K(M)$ передається одержувачу разом з вихідним повідомленням M. Отримувач повідомлення, знаючи, яка одностороння хеш-функція була застосована для отримання дайджесту, заново обчислює її, використовуючи розшифроване повідомлення M. Якщо значення отриманого дайджесту m і обчисленого дайджесту m' співпадають, то вміст повідомлення M не був модифікований. Знання дайджесту не дає можливості відновити вихідне повідомлення, але дозволяє перевірити цілісність даних.

Строга автентифікація, що базується на асиметричних алгоритмах.

У протоколах строгої автентифікації можуть бути використані асиметричні алгоритми з відкритими ключами. У цьому випадку генеруючій стороні потрібно продемонстрували знання секретного ключа одним із таких способів:

- Розшифрувати запит, зашифрований за допомогою відкритого ключа;
- Поставити свій цифровий підпис на запиті.

1. **Автентифікація з використанням асиметричних алгоритмів шифрування**

   $A \leftarrow B: h(r), B, P_A(r, B)$

   $A \rightarrow B: r$

Учасник B випадковим чином обирає число r та обчислює значення $x = h(r)$, а далі обчислює значення $e = P_A(r, B)$. Під P_Aрозуміють алгоритм асиметричного шифрування (наприклад, RSA), а під $h(r)$ - хеш-функцію. Учасник B відправляє учаснику A повідомлення. Учасник A розшифровує $e = P_A(r, B)$ та отримує значення r^1 та B^1, а також обчислює $x^1 = h(\, r^1)$. Після цього відбувається ряд порівнянь, які доводять що $x = x^1$ та що отриманий ідентифікатор B^1 дійсно вказує на учасника B. При успішному порівнянні A відправляє учаснику B значення r, отримавши яке B перевіряє це значення з тим, яке він відправив у першому повідомленні. Прикладом є модифікований протокол Нідхема і Шредера.

2. **Автентифікація, заснована на використанні цифрового підпису**

Введемо позначення

t_A, r_A, r_B −тимчасова мітка та випадкові числа відповідно

$S_A -$ підпис, сгенерований учасником A

$S_B -$ підпис, сгенерований учасником B

$cert_A -$ сертифікат відкритого ключа учасника A

$cert_B -$ сертифікат відкритого ключа учасника B

В якості прикладів наведемо такі протоколи аутентифікації:

1) Одностороння аутентифікація з застосуванням міток часу:

   $A \rightarrow B: cert_A, t_A, B, S_A(t_A, B)$

   Після прийняття даного повідомлення учасник B перевіряє правильність мітки часу t_A, отриманий ідентифікатор B і, використовуючи відкритий ключ з сертифікате $cert_A$, коректність цифрового підпису $S_A(t_A, B)$.

2) Одностороння аутентифікація з використанням випадкових чисел:

   $A \leftarrow B: r_B$

$A \rightarrow B: cert_A, r_A, B, S_A(r_A, r_B, B)$

Учасник B, отримавши повідомлення від учасника A, переконується, що саме він є адресатом повідомлення; використовуючи відкритий ключ учасника A, взятий з сертифікату $cert_A$, перевіряє коректність підпису $S_A(r_A, r_B, B)$ під числом r_A, отриманим у відкритому вигляді, числом r_B, яке було відіслано в першому повідомленні, та його ідентифікатором B. Підписане випадкове число r_A використовується для запобігання обертання атак з вибіркою відкритого тексту.

3) Двостороння аутентифікація з використанням випадкових чисел:

$A \leftarrow B: r_B$

$A \rightarrow B: cert_A, r_A, B, S_A(r_A, r_B, B)$

$A \leftarrow B: cert_B, \mathrm{A}, S_B(r_A, r_B, A)$

У даному протоколі обробка повідомлень 1 і 2 виконується так само, як і в попередньому протоколі, а повідомлення 3 обробляється аналогічно повідомленням 2.

2.3.3 Політики безпеки

Політика інформаційної безпеки — набір вимог, правил, обмежень, рекомендацій, які регламентують порядок інформаційної діяльності в організації і спрямовані на досягнення і підтримку стану інформаційної безпеки організації.

На основі політики безпеки будується керування, захист та розподіл критичної інформації в системі. Політика безпеки охоплює всі особливості процесу обробки інформації, визначаючи поведінку системи в різних ситуаціях.

- політика безпеки повинна визначати ресурси ІТС, що потребують захисту;
- мають бути сформульовані основні загрози для системи, персоналу та інформації різного рівня конфіденційності і вимоги до захисту від цих загроз;

- повинні бути визначені політики забезпечення конфіденційності, цілісності та доступності оброблюваної інформації;
- мають бути сформульовані правила розмежування доступу користувачів до ресурсів ІТС та інформації.

В теорії захисту інформації розглядають три наступні види політик безпеки інформаційних ресурсів:

- Дискретна політика безпеки
- Мандатна політика безпеки
- Рольова політика безпеки

Дискретна політика безпеки базується на дискреційному керуванні доступом до інформаційних ресурсів, тобто всі суб'єкти та об'єкти системи повинні бути однозначно ідентифікованими, а права доступу суб'єкта до об'єкта визначаються на основі деякого, зовнішнього відносно системи, правила доступу до системи і реалізуються шляхом безпосереднього звертання суб'єктів до об'єктів на основі певних атрибутів доступу. СЗІ повинна контролювати доступ тільки для ідентифікованих суб'єктів до об'єктів та для кожної пари суб'єкт-об'єкт.

Модель дискреційного керування може бути подана у вигляді матриці доступів Харрісона-Руззо-Ульмана. Матриця доступів – це матриця розміром $|S| \times |O|$, де рядки відповідають суб'єктам, а стовпці - об'єктам, при цьому кожен елемент матриці доступів $M[s, o] \subseteq R$ визначає права доступу суб'єкта s до об'єкту o, де $R -$ множина прав доступу.

Способи опису множини дозволених методів доступу суб'єкта до об'єкта можуть визначатися: списками дозволів (списки привілеїв) та списками керування доступом (access control list).

До переваг дискреційної політики безпеки можна віднести відносно просту реалізацію системи розмеження доступу. Цим обумовлений той факт, що більшість поширених сьогодні комп'ютерних систем забезпечують виконання вимог саме даної політики безпеки.

До недоліків дискреційної політики безпеки відноситься статичність визначених у ній правил розмежування доступу. Дана політика безпеки не враховує динаміку змін станів комп'ютерної системи. У загальному випадку при використанні даної політики безпеки перед системою захисту, яка при санкціонуванні доступу суб'єкта до об'єкта керується деяким набором правил, постає алгоритмічно нерозв'язна завдання - перевірити, чи приведуть його дії до порушення безпеки чи ні.

Тим не менш, в загальному випадку дискреційна політика розмежування доступу не дозволяє реалізувати ясну і чітку систему захисту інформації в комп'ютерній системі. Цим обумовлюється пошук інших, більш досконалих політик безпеки.

Мандатна політика безпеки базується на мандатному керуванні доступом до інформаційних ресурсів, що забезпечується виконанням наступних умов:

- усі суб’єкти та об’єкти повинні бути однозначно ідентифіковані;
- кожному об’єкту системи має бути присвоєна мітка певного рівня конфіденційності інформації, що визначає цінність інформації;
- кожному суб’єкту має бути присвоєна мітка рівня довіри системи до нього (рівень доступу);
- право доступу суб’єкта до об’єкта має визначатись на підставі порівняння їхніх міток.

Головне завдання мандатної політики безпеки полягає у запобіганні витоку інформації від об'єктів, що мають високий рівень доступу, до об'єктів із низьким рівнем доступу.

Модель мандатної політики в більшості випадків описується за використанням моделі Белла-Ла-Падули, формальний опис якої наведено у таблиці нижче (табл. 2.3).

Таблиця 2.3 – Формальне представлення моделі Белла-Ла-Падули

Елемент моделі	Опис
S	множина суб’єктів
O	множина об' єктів, така що S⊂O
R={r,w}	множина прав доступу, r- на читання,w-на запис
L={U,SU,S,TS}	множина рівнів конфіденційності інформаці, де: • U- unclassified, • SU- sensetive but unclassified, • S-secret, • TS-top secret
Λ=(L,≤,⊙,⊗)	решітка рівня конфіденційності, де: • ≤ – оператор, що визначає часткове нестроге відношення порядку для рівнів конфіденційності, • ⊙ – оператор найменшою верхньої межі
V	множина станів системи, що представлена у виді набору упорядкованих пар (F, M), де: • F:S∪O⟶L- функція рівнів конфіденційності, що ставить у відповідність кожному об'єкту і суб'єкту в системі певний рівень конфіденційності, • M- матриця поточних прав доступу
$\Sigma = (v_0, R, T)$	В моделі Белла-ЛаПадули задається в наведеному вигляді та характеризується наступним: • v_0 – початковий стан системи, • R – множина прав доступу до об′єктів, • $T: V \times R \to V$ – функція переходу, що переводить систему з одного стану в наступний при виконанні запитів.

Нижче наведено основні принципи, що характеризують модель Белла-ла-Падули:

Стан v називається досяжним в системі $\Sigma = (v_0, R, T)$, якщо існує послідовність $\{(r_0, v_0), \dots, (r_{n-1}, v_{n-1}), (r_n, v_n)\}: T(r_i, v_i) = v_{i+1} \quad \forall i = \overline{0, n-1}$. Початковий стан v_0 є досяжним за визначенням.

Стан системи (F, M) називається безпечним за читанням, якщо для кожного суб'єкта, який здійснює в цьому стані доступ за читанням до об'єкта, рівень безпеки суб'єкта домінує над рівнем безпеки об'єкта:

$$\forall s \in S, \forall o \in O, r \in M[s, o] \rightarrow F(o) \leq F(s)$$

Стан системи (F, M) називається безпечним по запису у випадку, якщо для кожного суб'єкта, який здійснює в цьому стані доступ по запису до об'єкта, рівень безпеки об'єкта домінує над рівнем безпеки суб'єкта:

$$\forall s \in S, \forall o \in O, w \in M[s, o] \rightarrow F(s) \leq F(o)$$

Стан (F, M) називається безпечним, якщо воно безпечне за читанням та по запису.

Система $\Sigma = (v_0, R, T)$ безпечна тоді й тільки тоді, коли виконані наступні умови:

1) початковий стан v_0 безпечний;
2) для ∀ стану v, досяжного із v_0 за допомогою кінченої послідовності запитів із R, таких що

   $T(v, r) = v^*, v = (F, M), v^* = (F^*, M^*)$ $\forall s \in S$, $\forall o \in O$ виконані умови:

   1) Якщо $r \in M^*[s, o]$ та $r \notin M[s, o]$, то $F^*(o) \leq F^*(s)$

   2) Якщо $r \in M[s, o]$ та $F^*(s) < F^*(o)$, то $r \notin M^*[s, o]$

   3) Якщо $w \in M^*[s, o]$ та $w \notin M[s, o]$, то $F^*(s) \leq F^*(o)$

   4) Якщо $w \in M[s, o]$ та $F^*(o) < F^*(s)$, то $w \notin M^*[s, o]$

Тобто, якщо інформаційна система починає роботу з безпечного стану і перехід з поточного стану у новий стан є безпечним, то всі стани системи безпечні.

Для систем мандатного розмежування доступу завдання перевірки безпеки є алгоритмічно вирішуваною. Крім того, порівняно з комп'ютерними системами, побудованими на основі дискреційної політики безпеки, для систем, що реалізують мандатну політику, характерна більш висока ступінь надійності.

Проте мандатна модель Белла-ЛаПадули має суттєві недоліки: декласифікація (тобто зміна рівня конфіденційності об’єкту за бажанням суб’єкта з високим рівнем доступу), віддалене читання у розподілених системах, високі вимоги до обчислювальних ресурсів і складність практичної реалізації такої системи.

Рольова політика безпеки базується на дискретній політиці безпеки та є її удосконаленим варіантом. Згідно з цією політикою, усі суб’єкти і об’єкти повинні бути однозначно ідентифікованими, визначено набір ролей у системі та кожній ролі встановлено певний обсяг повноважень, доступ суб’єктів до об’єктів здійснюється на підставі певних правил в рамках певної ролі.

Класичне поняття “суб’єкт” заміщується поняттями “користувач” і “роль”. Користувач – це людина, яка працює з системою і виконує певні службові обов’язки. Роль – це активно діюча в системі абстрактна сутність, з якою асоційований обмежений набір повноважень, що необхідні для здійснення певної діяльності.

Формальний опис рольової моделі політики наведено у Таблиці 2.4 нижче.

Таблиця 2.4 – Формальне представлення рольвої моделі розмежування доступу

Елемент моделі	Опис
1	2
U	множина користувачів
R	множина ролей
P	множина повноважень на доступ до об’єктів, що може бути подана у вигляді матриці доступу
S	множина сеансів роботи користувача із системою

Продовження таблиці 2.4

1	2
PA⊆P×R	відображає множину повноважень на множину ролей, встановлюючи для кожної ролі набір наданих їй повноважень
UA⊆U×R	відображає множину користувачів на множину ролей, встановлюючи для кожного користувача набір доступних йому ролей

Правила керування доступом визначаються наступним чином:

- $user: S \to U$ – для кожного сеансу s ця функція визначає користувача u, який здійснює цей сеанс роботи із системою: $user(s) = u$;
- $roles: S \to R$– для кожного сеансу s ця функція визначає набір ролей з множини R, що можуть бути одночасно доступні користувачу u у цьому сеансі: $roles(s) = \{r \mid user(s), r\} \in UA$;
- $permissios: S \longrightarrow P$ – для кожного сеансу s ця функція задає набір доступних у ньому повноважень, який визначається як сукупність повноважень усіх ролей, що беруть участь у цьому сеансі: $permissios(s) = \{p \mid (p, r)\} \in PA$;

Критерій безпеки рольової моделі: система вважається безпечною, якщо будь-який користувач системи u, що працює в сеансі s, може здійснити дії, які вимагають повноважень p, тільки у тому випадку, коли $p \in permissios(s)$.З цього випливає, що керування доступом здійснюється переважно не шляхом призначення повноважень ролям, а шляхом завдання відношення UA, яке призначає ролі користувачам, і функції $roles$, що визначає доступний у сеансі набір ролей.

Ця політика відрізняється від інших політик своєю гнучкістю. Її активно використовують у системах управління базами даних, де встановлено чіткі повноваження й обов'язки адміністраторів і користувачів інформаційної системи. На основі цієї політики часто реалізують інші політики, зокрема й мандатну.

Тож організація повинна чітко спланували:

- як користувачі будуть отримувати доступ та користуватися ресурсами
- де будуть розміщатися користувачі: тільки в корпоративній мережі чи будуть мати доступ до хмарного сервісу бази даних
- категорії користувачів (штатні/позаштатні співробітники, інше)

Від цього залежить подальша реалізація таких механізмів системи захисту як ідентифікація, автентифікація та авторизація.

2.3.4 Моніторинг та аудит

Провайдери хмарних сервісів зазвичай самі надають необхідні інструменти аудиту та моніторингу, проте на випадок конфліктів організація повинна застосовувати власні протоколи аудиту. Такі протоколи дають цінні відомості про взаємодію співробітників організації з конкретним хмарним сервісом, вчасно визначають проблеми конфігурацій та політик, відповідні порушення, надають змогу формувати звіти про проблеми. Також організація-споживач може скористатися послугами стороннього брокера хмарних сервісів для ведення незалежного протоколу споживання хмарного сервісу.

У DBaaS з метою забезпечення високого рівня доступності та надмірності, дані клієнтів, як правило реплікуються між кількома ЦОД в декількох місцях, що призводить до нестатичного середовища, де споживачі не мають ніякої видимості або доступності фізичної інфраструктури. Моніторинг бази даних і аудит дає змогу постійно (і надійно) вести записи і звіти про всі події, що відбуваються в СУБД (наприклад, генерування звітів про те, як, коли і ким різні об'єкти були запитані або змінені). Сильний аудит і моніторинг бази даних забезпечує повну прозорість у діяльності бази даних незалежно від його місця розташування та є надзвичайно важливим для хмарних сервісів бази даних.

Можливості аудиту забезпечують відповідальність користувачів за свої дії, перевірку дотримання політики безпеки, а також можуть бути використані при проведенні розслідувань.

Доцільно враховувати наступні моменти при організації системи аудиту:

- Журнали реєстрації подій повинні зберігатися захищеним чином
- Слід використовувати надійні інструменти роботи з файлами журналів реєстрації подій, які зберігають розмір файлів журналів
- Журнали реєстрації подій повинні бути захищені від зміни неуповноваженими особами
- Слід навчати відповідний персонал правильним процедурам аналізу даних в журналах реєстрації подій
- Необхідно забезпечити гарантії того, що видалення журналів реєстрації подій доступно тільки адміністраторам
- Журнали реєстрації подій повинні включати в себе дії всіх високопрівілегованих облікових записів (корінь, адміністратор)

2.3.5 Криптографічний захист даних

Користувачі зберігають свої дані на серверах хмарного провайдеру, що призводить до втрати контролю над даними. Фізичне зберігання даних на сервері може призводити до різних проблем безпеки та конфіденційності, наприклад, неавторизований доступ робітників хмарного сервісу та зловмисників. Також сервери повинні надавати ефективні механізми ізоляції та зберігання даних користувачів.

2.3.6 Обробка шифрованих даних у СКБД

Розглянемо типові задачі, які актуальні при роботі з конфіденційними даними у публічній хмарі та протоколи, які забезпечують ефективність та секретність як обчислюваних даних, так і результатів операцій з ними.

Існує велика потреба в створенні такої взаємодії з сервером бази даних, при якій можна не тільки зберігати на ньому дані споживача у зашифрованому виді, але й дозволити серверу проводити необхідні обчислення над цими даними, при цьому не дізнавшись ніякої додаткової інформації.

Існує два протоколи, які зараз використовуються при звертанні до баз даних.

Приватне отримання даних (Private Information Retrieval). Цей протокол запобігає провайдеру хмарних обчислень використовувати схеми доступу до конфіденційних даних споживача. Схеми протоколу PIR є інтерактивними двопартійними протоколами між клієнтом і сервером та намагаються виконати наступну задачу: існує база даних із n біт. Клієнт хоче дістати біт номер i так, щоб база даних, яка містить всі n біт, не дізналася ніякої інформації про те, який біт вибрав клієнт.

- Найпростіший спосіб рішення полягає в наступному: клієнт створює програмний код, що буде шифрувати дані, та відправляє зашифровані дані на сервер для зберігання. Для того, щоб дістати необхідний біт i , клієнт закачує всю базу із n біт на клієнтську сторону, розшифровує дані, проводить необхідні обчислення над i, знову зашифровує дані та відправляє назад на сервер. Цей спосіб забезпечує безпеку тільки клієнта і не розкриває серверу, які саме дані цікавлять клієнта. Але він є дуже неефективним, трудомістким, а головне – не відповідає ідеї хмарних послуг. А при доступі до хмарної бази з пристроїв з обмеженими обчислюваними ресурсами це стає справжньою проблемою.

- Інший шлях – використання PIR-протоколу, де клієнт робить запит (функцію) серверу бази даних. Останній бере цю функцію, докладає її до всієї сукупності бази даних і отримує відповідь, яка висилається назад клієнтові. Існують наступні умови цієї передачі: довжина запиту (функції) та відповіді повинна бути багато менше ніж довжина бази даних n; клієнт повинен для будь-якого біту i послати такий запит, щоб біт i був вірно отриманий; сервер не може нічого дізнатися з приводу біту i.

Забудькувата передача (Oblivious transfer protocol, OT). Це протокол передачі даних, в якому сервер передає можливі частини інформації клієнту, але не запам'ятовує (є забудькуватим), які частини були передані, якщо взагалі були. На додачу до попереднього протоколу PIR, протокол OT гарантує і безпеку серверу. Повинні виконуватися дві умови: по-перше, клієнт повинен отримати саме ті дані, які він хоче; по-друге, сервер не повинен відправити будь-яких інших додаткових даних. Описання OT протоколу було представлено Мішелем Рабіним у 1981 році: OT дозволяє серверу відправляти клієнтові повідомлення з ймовірністю ½ і в той же час не запам'ятовувати, було чи ні отримано повідомлення клієнтом. Технічна реалізація протоколу близька до криптосистеми Рабіна:

- На початку протоколу сервер володіє наступними даними: пара великих простих чисел p і q (таких, що складний модуль $N = pq$ та їх добуток – важка RSA-задача); згенерована експонента e така, що $\text{НОД}\big(e, \varphi(N)\big) = 1$; повідомлення серверу m – це елемент групи Z_N.
- Сервер відправляє клієнту публічні дані N, e, m^e.
- Клієнт вибирає деяку випадкову величину $x \bmod N$, обчислює та відправляє серверу $x^2 \bmod N$. Так як $\text{НОД}(x, N) = 1$, то з великою ймовірністю пересланий елемент $x^2 \bmod N$ буде мати 4 квадратні корені.

- Сервер знаходить квадратний корень y від $x^2\ mod\ N$ та відправляє його назад клієнтові.
- Далі можливі два випадки:
  - Якщо y не є «$xmodN$» і не є «$-xmodN$», тоді клієнт може факторизувати N і розшифрувати m^e для отримання m.
  - В іншому випадку, цей квадратний корінь не дає ніякої інформації про повідомлення m.

Тобто клієнт має можливість розшифрувати повідомлення з ймовірністю 50 %, при цьому сервер не знає, чи вдалося клієнту розшифрувати повідомлення.

Найбільш популярною операцією з даними у хмарі є операція пошуку на сервері-сховищі, де дані зберігаються у зашифрованому виді. Традиційно користувач скачує усі зашифровані дані на локальну машину, розшифровує їх та все потім проводить пошук у відкритому тексті. Проте ця схема суперечить поняттю хмарних обчислень та надання послуги бази даних як сервісу. Тож для вирішення цієї проблеми розглянемо наступні алгоритми шифрування, що дозволяють серверу обчислювати зашифровані дані та видавати результат, який при розшифровці співпадає з результатом, який мав би бути отриманий при проведенні обчислень над відкритим текстом.

Протокол забудькуватої передачі «1-із-2» (OT 1-out-of-2). Цей варіант протоколу був розроблений з метою створення протоколу конфіденційного обчислення. Він реалізує обмін даними між клієнтом і сервером бази даних та базується на криптосистемі Diffie-Hellman Integrated Encryption Scheme.

На початку протоколу сервер має дві бітові строки (повідомлення) m_0 та m_1 однакової довжини N, а клієнт має певний біт b та хоче отримати повідомлення m_b так, щоб сервер не дізнався нічого про біт b, в той же час сервер повинен бути впевнений, що клієнт отримав тільки одне з двох повідомлень і нічого не дізнався про друге.

- Сервер має два повідомлення m_0 та m_1 і хоче відправити одне із них клієнту, але не має дізнатися яке саме повідомлення отримає клієнт.
- Сервер генерує пару RSA-ключів за модулем N, публічну експоненту e
  - та секретну експоненту d.
- Сервер генерує два випадкові значення x_0 і x_1, та відправляє їх клієнтові разом з N, e.
- Клієнт обирає біт b, що дорівнює або 0, або 1, а також обирає або перший або другий x_b.
- Клієнт генерує випадкове значення k та шифрує x_b розраховуючи $v = (x_b + k^e) mod N$, які відправляє назад серверу.
- Сервер не знає, яке з x_0 і x_1 обрав клієнт, намагається розшифрувати обидва випадкових повідомлення та отримує два значення k: $k_0 = (v - x_0)^d mod\ N$ та $k_1 = (v - x_1)^d mod\ N$, одне з яких буде відповідати обраному клієнтом значенню k і коректно розшифроване, а інше буде випадковим значенням, яке не розкриває ніякої інформації про значення k.
- Сервер шифрує обидва секретних повідомлення з кожним ймовірним ключем $m'_0 = m_0 + k_0$, $m'_1 = m_1 + k_1$ та відправляє їх клієнтові.
- Клієнт знає, яке з двох отриманих повідомлень може бути розшифроване за допомогою k, та отримує можливість розшифрувати лише одне повідомлення $m_b = m'_b - k$.

Висновки до розділу 2

Захист інформаційних ресурсів, що обробляються та зберігаються в хмарних СКБД, базується на наступних аспектах: захист каналів зв’язку, забезпечення процесу автентифікації, застосування політик безпеки, наявність процесу моніторингу та аудиту, криптографічного захисту інформації, а також обробки даних в СКБД. Дані аспекти мають бути застосовані к коплексі, для забезпечення повного покриття питань захисту інформації.

Для побудови моделі системи засисту інформації треба визначити властиві даному типу систем вразливості, перелік загроз, які можуть експлуатувати відповідні вразливості, агенти загроз. Далі необхідно встановити пари загроз та вразливостей, визначити для них агента загроз та навести перелік відповідних контролів (заходів безпеки), що забезпечить прозорість їхного використання для забезпечення захисту інформації. Дані контролі можуть бути реалізовані за допомогою використання різних механізмів, процесів та засобів забезпечення безпеки, порівняльний аналіз яких проведено в даному розділі. На основі результатів даного аналізу можна надати рекомендації щодо впровадження контролів в рамках моделі СЗІ в хмарних СКБД.

3 МОДЕЛЬ ЗАХИСТУ ДАНИХ ДЛЯ ХМАРНИХ СКБД

Побудова моделі системи захисту даних, застосовної для хмарних СКБД (DataBase-as-a-Service), базується на вимогах шодо захисту інфомації в залежності від класифікації згідно діючого законодавства, вимогах міжнародних стандартів щодо систем захисту інформації, результатах аналізу найактуальніших загроз та вразливостей, які є застосовними до хмарних сервісів, а також на результатах аналізу заходів та засобів безпеки, що забезпечують повне покриття питань інформаційної безпеки для хмарних СКБД.

В якості активу розглядається інформація організації, яка обробляється та зберігається у хмарній СКБД. Дана інформація класифікована як конфіденційна, а також частина інформації як службова (інформація внутрішнього користування), тобто дана інформація є інформацією з обмеженим доступом.

Для забезпечення належного рівня безпеки інформації при побудові моделі системи захисту інформації в хмарних СКБД збережено відповідну послідовність кроків:

- Встановлено перелік вразливостей, властивих у відношенні до хмарних СКБД та згруповано їх по категоріям відповідно до аспектів захисту;
- Встановлено перелік загроз, що можуть експлуатувати вразливості хмарних СКБД та згруповано їх по категоріям відповідно до аспектів захисту;
- Співставлено пари вразливостей та загроз, які можуть бути реалізовані при експлуатації відповідних вразливостей;
- Встановлено перелік агентів загроз, здатних до проведення атак різного роду в залежності від наявних в них ресурсів та мотивації;
- До кожної пари з вразливостей та загроз наведено всі властиві засоби і заходи засисту;
- Надано рекоменції щодо застосування наведених методів захисту.

Перелік вразливостей, застосовних до хмарних систем керування базами даних наведено нижче у Таблиці 3.1:

Таблиця 3.1 – Вразливості, властиві хмарним системам керування базами даних

id	**Аспект ІБ**	**Вразливість**	**Застосовні загрози**
1	2	3	4
1.	Ідентифікація та автентифікація	Система не однозначно ідентифікує та не перевіряє користувачів чи процеси	1, 2, 6, 8, 9
2.		Система розкриває будь-які автентифікаційні дані під час процесу автентифікації	1, 6, 8, 9
3.		Система не впроваджує політику паролів (складність пароля, мінімальний термін дії та закінчення терміну дії, історія, межа блокування облікового запису, тривалість блокування облікового запису)	1, 2, 6, 8, 9
4.		Система не забезпечує нагадування для користувача про обов'язкову зміну пароля	1, 2, 6, 8, 9
5.	Управління доступом	Права доступу користувачів не переглядаються через визначені регулярні інтервали часу та після будь-яких змін	1, 7, 8, 9, 10
6.		Система не однозначно авторизує користувачів виконувати дії у відношенні активів	1, 7, 8, 9
7.	Обробка та захист даних	Відсутність або неповнота систем моніторингу	1, 2, 4, 5, 6, 7, 8, 9
8.		Перевірки безпеки коду не проводяться для того, не встановлюється наявність належних елементів контролю безпеки та того, що вони працюють належним чином (як це передбачено та у всіх відповідних випадках)	8
9.		Постачальник сервісу має доступ до клієнтських СКБД	1, 2, 5, 6, 9

Продовження таблиці 3.1

1	2	3	4
10	Обробка та захист даних	Мережа, система не захищає передані дані (у тому числі клієнт-серверний зв'язок)	1, 2, 6, 9
11.		Відсуність шифрування СКБД	1, 2, 3, 6, 8, 9
12.	Логування та моніторинг	Відсутність логування доступу в СКБД	1, 6, 7, 9
13.		Інциденти безпеки не пересилаються на сервер SIEM	1, 4, 5, 6, 7, 9
14.	Патч-менеджмент	Патчі, що стосуються безпеки, для системи не оцінюються та не встановлюються протягом 30 днів після їх випуску (якщо вони пройшли перевірки валідації)	1, 2, 5, 6
15.		Патчі, які стосуються безпеки, не тестуються перед їх встановленням	12
16.	Управління вразливостями	Не виконується сканування вразливостей для мереж, систем з регулярними інтервалами	1, 2, 5, 6
17.		Тестування на проникнення не виконується для мережі та систем щонайменше один раз на рік	1, 2, 5, 6
18.	HR	Помилки персоналу, недбалість, порушення внутрішніх правил	3, 5, 7, 9
19.	Відновлення після збоїв	Резервне копіювання інформації не проводиться з визначеною частотою та резервні копії не зберігаються належним чином	8, 13
20.		Резевні копії інформації не перевіряються з заданою частотою відповідно до погодженої резервної політики для перевірки цілісності та доступності інформації	8, 13
21.		Відсутній план для відновлення після збоїв	11, 8, 13
22.		План відновлення після збоїв для системи не перевіряється через визначені регулярні інтервали	11, 8, 13

Продовження таблиці 3.1

1	2	3	4
23.	Відновлення після збоїв	Recovery Time Objective (RTO) та Recovery Point Objective (RPO) не визначені	11, 8, 13
24.	Фізична безпека	Відсутність логування системаи контролю доступу для усіх спроб (успішних та невдалих) фізичного доступу до приміщення з інформацією про ідентифікатор, датою та часом доступу	9, 10
25.		Система контролю доступу не зберігає інформацію про події протягом 3 місяців	9, 10
26.		Відсутнє резервне джерело живлення для системи контролю доступу для забезпечення безперебійного живлення в разі надзвичайної ситуації протягом щонайменше 8 годин	9, 10
27.		Приміщення не обладнані системами сигналізації	9, 10
28.		Вхідні двері в приміщення не контролюються камерою відеоспостереження 24/7	9, 10
29.		Приміщення не обладнано системою пожежної сигналізації	11
30.		Відсутні системи заземлення та громовідводу	11
31.		Відсутність щонайменше двох джерел живлення для повсякденного використання	11
32.		Не здійснюється автоматичний перехід на використання джерел бесперебійного живлення при втраті основного джерела	11
33.		Не проводиться тестування бесперебійного джерела живлення як мінімум один раз на рік	11

Продовження таблиці 3.1

1	2	3	4
34.	Фізична безпека	Датчики затоплення не встановлені або не забезпечують автоматичного попередження в разі затоплення	11
35.		Температурні датчики не встановлені або не забезпечують автоматичного попередження при підвищенні температури до критичного рівня	11
36.	Правова сфера	Відсутність або недостатність умов інформаційної безпеки у контрактах з третіми сторонами	13
37.		Відсутність процесу відстеження змін у законодавстві	14
38.	Менеджмент	Відсутність проведення регулярних аудитів	13, 14
39.		Недостатність ресурсів	14
40.	Обробка та захист даних	Відсутність системи контролю версій	3

Перелік загроз, застосовних до хмарних систем керування базами даних наведено нижче у Таблиці 3.2:

Таблиця 3.2 – Перелік загроз, застосовних до хмарних систем керування базами даних

id	**Аспект ІБ**	**Загроза**	**Застосовність до врасливостей**
1	2	3	4
1.	Кібербезпека	Хакерські атаки, веб-атаки, несанкціонований доступ до мережі, системи	1, 2, 3, 4, 5, 6, 7, 9, 10, 11, 12, 14, 16, 17

Продовження таблиці 3.2

1	2	3	4
2.	Кібербезпека	Модифікація мережевого трафіку, незахищені канали зв'язку	1, 3, 4, 7, 9, 10, 11, 14, 16, 17
3.		Зловмисні дії інсайдера	1, 2, 3, 4, 5, 6, 7, 9, 10, 12, 13, 14, 16, 17
4.		DDoS attack	7, 13
5.		Впровадження шкідливого коду (вірусів, програмного забезпечення тощо)	7, 9, 13, 14, 16, 17, 18
6.		Несанкціоноване отримання інформації аутентифікації, підвищення привілеїв	2, 3, 4, 7, 9, 10, 12, 13, 14, 16, 17
7.		Несанкціонована модифікація, встановлення програмного забезпечення	5, 6, 7, 12, 13, 18
8.		Несанкціонована модифікація програмного забезпечення, інформації з обмеженим доступом	1, 2, 3, 4, 5, 6, 7, 8, 19, 21, 22, 23
9.		Розкриття або крадіжка інформації з обмеженим доступом	1, 2, 3, 4, 5, 6, 7, 10, 9, 10, 11, 15, 12, 13, 18, 24, 25, 26, 27, 28
10	Фізична безпека	Крадіжка активів	5, 24, 25, 26, 27, 28
11.		Руйнування, втрата, відсутність обладнання, комунікаційних зв'язків, послуг, інформації внаслідок природних чи техногенних	19, 20, 21 ,22, 23, 29, 30, 31, 32, 33, 34, 35

Продовдення таблиці 3.2

1	2	3	4
11		катастроф, війни, масових розладів, втрати потужності чи системи кондиціонування	
12.	Менеджмент	Непередбачуваний ефект від зміни інформації з обмеженим доступом, програмного забезпечення, обладнання	15
13.	Правова сфера	Порушення договірних зобов'язань, NDA з постачальниками, клієнтами	19, 36, 38
14.		Недотримання українського, міжнародного законодавства, внутрішніх політик	37, 38, 38

Перелік агентів загрози, що зацікавленні в проведенні атаки на хмарні СКБД наведено нижче у Таблиці 3.3:

Таблиця 3.3 – Агенти загрози

Агент загрози
Інсайдер
Хакер

Перелік контролів, спрямованих на захист інформації в хмарних СКБД наведено нижче у Таблиці 3.4:

Таблиця 3.4. Перелік контролів, спрямованих на захист інформації в хмарних СКБД

id	**Аспект ІБ**	**Заходи безпеки**
1.		
2.		
3.		
4.		
5.		
6.		

Далі в нижченаведеній Таблиці 3.5 у матричному вигляді представлена модель системи захисту інформації для хмарних СКБД, що являє собою пари загроз та вразливостей, агентів загроз, та заходів безпеки, спрямованих на захист інформаційних ресурсів. Дана модель забезпечує повне покриття питань інформаційної безпеки для хмарних систем керування базами даних необхідними заходами безпеки (або контролями).

Таблиця 3.5 Матрична модель системи захисту інформації в хмарних СКБД

id	**Вразливість**	**Загроза**	**Агент загрози**	**Заходи безпеки**
1	Система не однозначно ідентифікує та не перевіряє користувачів чи процеси			
2	Система не однозначно ідентифікує та не перевіряє користувачів чи процеси			
3	Система не однозначно ідентифікує та не перевіряє користувачів чи процеси			
4	Система не однозначно ідентифікує та не перевіряє користувачів чи процеси			

5	Система не однозначно ідентифікує та не перевіряє користувачів чи процеси			
6	Система розкриває будь-які автентифікаційні дані під час процесу автентифікації			
7	Система розкриває будь-які автентифікаційні дані під час процесу автентифікації			
8	Система розкриває будь-які автентифікаційні дані під час процесу автентифікації			
9	Система розкриває будь-які автентифікаційні дані під час процесу автентифікації			
10	Система не впроваджує політику паролів (складність пароля, мінімальний термін дії та закінчення терміну дії, історія, межа блокування			

	облікового запису, тривалість блокування облікового запису)			
11	Система не впроваджує політику паролів (складність пароля, мінімальний термін дії та закінчення терміну дії, історія, межа блокування облікового запису, тривалість блокування облікового запису)			
12	Система не впроваджує політику паролів (складність пароля, мінімальний термін дії та закінчення терміну дії, історія, межа блокування облікового запису, тривалість блокування облікового запису)			
13	Система не впроваджує політику паролів (складність пароля, мінімальний термін дії та закінчення терміну дії, історія, межа блокування			

	облікового запису, тривалість блокування облікового запису)			
14	Система не впроваджує політику паролів (складність пароля, мінімальний термін дії та закінчення терміну дії, історія, межа блокування облікового запису, тривалість блокування облікового запису)			
15	Система не забезпечує нагадування для користувача про обов'язкову зміну пароля			
16	Система не забезпечує нагадування для користувача про обов'язкову зміну пароля			
17	Система не забезпечує нагадування для користувача про обов'язкову зміну пароля			
18	Система не забезпечує нагадування для користувача про обов'язкову зміну пароля			

19	Система не забезпечує нагадування для користувача про обов'язкову зміну пароля			
20	Права доступу користувачів не переглядаються через визначені регулярні інтервали часу та після будь-яких змін			
21	Права доступу користувачів не переглядаються через визначені регулярні інтервали часу та після будь-яких змін			
22	Права доступу користувачів не переглядаються через визначені регулярні інтервали часу та після будь-яких змін			
23	Права доступу користувачів не переглядаються через визначені регулярні інтервали часу та після будь-яких змін			
24	Права доступу користувачів не переглядаються через			

	визначені регулярні інтервали часу та після будь-яких змін			
25	Система не однозначно авторизує користувачів виконувати дії у відношенні активів			
26	Система не однозначно авторизує користувачів виконувати дії у відношенні активів			
27	Система не однозначно авторизує користувачів виконувати дії у відношенні активів			
28	Система не однозначно авторизує користувачів виконувати дії у відношенні активів			
29	Відсутність або неповнота систем моніторингу			

30	Відсутність або неповнота систем моніторингу			
31	Відсутність або неповнота систем моніторингу			
32	Відсутність або неповнота систем моніторингу			
33	Відсутність або неповнота систем моніторингу			
34	Відсутність або неповнота систем моніторингу			
35	Відсутність або неповнота систем моніторингу			
36	Відсутність або неповнота систем моніторингу			
37	Перевірки безпеки коду не проводяться для того, не встановлюється наявність належних елементів контролю безпеки та того, що вони працюють належним чином			

	(як це передбачено та у всіх відповідних випадках)			
38	Постачальник сервісу має доступ до клієнтських СКБД			
39	Постачальник сервісу має доступ до клієнтських СКБД			
40	Постачальник сервісу має доступ до клієнтських СКБД			
41	Постачальник сервісу має доступ до клієнтських СКБД			
42	Постачальник сервісу має доступ до клієнтських СКБД			
43	Мережа, система не захищає передані дані (у тому числі клієнт-серверний зв'язок)			
44	Мережа, система не захищає передані дані (у тому числі клієнт-серверний зв'язок)			
45	Мережа, система не захищає передані дані (у тому числі клієнт-серверний зв'язок)			

46	Мережа, система не захищає передані дані (у тому числі клієнт-серверний зв'язок)			
47	Відсуність шифрування СКБД			
48	Відсуність шифрування СКБД			
49	Відсуність шифрування СКБД			
50	Відсуність шифрування СКБД			
51	Відсуність шифрування СКБД			
52	Відсуність шифрування СКБД			
53	Відсутність логування доступу в СКБД			
54	Відсутність логування доступу в СКБД			
55	Відсутність логування доступу в СКБД			
56	Відсутність логування доступу в СКБД			
57	Інциденти безпеки не пересилаються на сервер SIEM			
58	Інциденти безпеки не пересилаються на сервер SIEM			

59	Інциденти безпеки не пересилаються на сервер SIEM			
60	Інциденти безпеки не пересилаються на сервер SIEM			
61	Інциденти безпеки не пересилаються на сервер SIEM			
62	Інциденти безпеки не пересилаються на сервер SIEM			
63	Патчі, що стосуються безпеки, для системи не оцінюються та не встановлюються протягом 30 днів після їх випуску (якщо вони пройшли перевірки валідації)			
64	Патчі, що стосуються безпеки, для системи не оцінюються та не встановлюються протягом 30 днів після їх випуску (якщо вони пройшли перевірки валідації)			

65	Патчі, що стосуються безпеки, для системи не оцінюються та не встановлюються протягом 30 днів після їх випуску (якщо вони пройшли перевірки валідації)			
66	Патчі, що стосуються безпеки, для системи не оцінюються та не встановлюються протягом 30 днів після їх випуску (якщо вони пройшли перевірки валідації)			
67	Патчі, які стосуються безпеки, не тестуються перед їх встановленням			
68	Не виконується сканування вразливостей для мереж, систем з регулярними інтервалами			
69	Не виконується сканування вразливостей для мереж,			

	систем з регулярними інтервалами			
70	Не виконується сканування вразливостей для мереж, систем з регулярними інтервалами			
71	Не виконується сканування вразливостей для мереж, систем з регулярними інтервалами			
72	Тестування на проникнення не виконується для мережі та систем щонайменше один раз на рік			
73	Тестування на проникнення не виконується для мережі та систем щонайменше один раз на рік			
74	Тестування на проникнення не виконується для мережі та			

	систем щонайменше один раз на рік			
75	Тестування на проникнення не виконується для мережі та систем щонайменше один раз на рік			
76	Помилки персоналу, недбалість, порушення внутрішніх правил			
77	Помилки персоналу, недбалість, порушення внутрішніх правил			
78	Помилки персоналу, недбалість, порушення внутрішніх правил			
79	Помилки персоналу, недбалість, порушення внутрішніх правил			
80	Резервне копіювання інформації не проводиться з визначеною частотою та			

	резервні копії не зберігаються належним чином			
81	Резервне копіювання інформації не проводиться з визначеною частотою та резервні копії не зберігаються належним чином			
82	Резевні копії інформації не перевіряються з заданою частотою відповідно до погодженої резервної політики для перевірки цілісності та доступності інформації			
83	Резевні копії інформації не перевіряються з заданою частотою відповідно до погодженої резервної політики для перевірки цілісності та доступності інформації			
84	Відсутній план для відновлення після збоїв			

85	Відсутній план для відновлення після збоїв			
86	Відсутній план для відновлення після збоїв			
87	План відновлення після збоїв для системи не перевіряється через визначені регулярні інтервали			
88	План відновлення після збоїв для системи не перевіряється через визначені регулярні інтервали			
89	План відновлення після збоїв для системи не перевіряється через визначені регулярні інтервали			
90	Recovery Time Objective (RTO) та Recovery Point Objective (RPO) не визначені			

91	Recovery Time Objective (RTO) та Recovery Point Objective (RPO) не визначені			
92	Recovery Time Objective (RTO) та Recovery Point Objective (RPO) не визначені			
93	Відсутність логування системаи контролю доступу для усіх спроб (успішних та невдалих) фізичного доступу до приміщення з інформацією про ідентифікатор, датою та часом доступу			
94	Відсутність логування системаи контролю доступу для усіх спроб (успішних та невдалих) фізичного доступу до приміщення з інформацією про ідентифікатор, датою та часом доступу			

95	Система контролю доступу не зберігає інформацію про події протягом 3 місяців			
96	Система контролю доступу не зберігає інформацію про події протягом 3 місяців			
97	Приміщення не обладнані системами сигналізації			
98	Приміщення не обладнані системами сигналізації			
99	Вхідні двері в приміщення не контролюються камерою відеоспостереження 24/7			
100	Вхідні двері в приміщення не контролюються камерою відеоспостереження 24/8			
101	Приміщення не обладнані системами сигналізації			
102	Відсутні системи заземлення та громовідводу			

103	Відсутність щонайменше двох джерел живлення для повсякденного використання			
104	Не здійснюється автоматичний перехід на використання джерел бесперебійного живлення при втраті основного джерела			
105	Не проводиться тестування бесперебійного джерела живлення як мінімум один раз на рік			
106	Датчики затоплення не встановлені або не забезпечують автоматичного попередження в разі затоплення			
107	Температурні датчики не встановлені або не забезпечують автоматичного попередження при підвищенні			

	температури до критичного рівня			
108	Відсутність або недостатність умов інформаційної безпеки у контрактах з третіми сторонами			
109	Відсутність процесу відстеження змін у законодавстві			
110	Відсутність проведення регулярних аудитів			
111	Відсутність проведення регулярних аудитів			
112	Недостатність ресурсів			
113	Відсутність системи контролю версій			
114	Система не однозначно ідентифікує та не перевіряє користувачів чи процеси			

Висновки до розділу 3

В ході виконання дваної кваліфікаційної роботи було побудовано матричну модель системи захисту інформації в хманих СКБД на основі аналізу вимог до захисту інформації в залежності від її класифікації згідно до вимог діючого законодавства. Було виконано аналіз архітектури хмарних сервісів, розглянуто архітектуру та характеристики хмарних СКБД.

Для побудови моделі системи засисту інформації було визначено властиві даному типу систем вразливості, перелік загроз, які можуть експлуатувати відповідні вразливості, а також можливих агентів загроз. Далі було встановлено пари загроз та вразливостей, визначено для них агента загроз та наведено перелік відповідних контролів (заходів безпеки), що забезпечує прозорість їхного використання в цілях захисту інформації. Дані контролі можуть бути реалізовані за допомогою використання різних механізмів, процесів та засобів забезпечення безпеки, для яких було проведено порівняльний аналіз та наведено їх пріоритизацію до використання. Результати даної пріоритизації використано при співставленні заходів безпеки та рекомендацій щодо їх використання.

ВИСНОВКИ

В зв’язку зі стрімким переносом зберігання та обробки даних в хмарні сервіси виникає необхідність регламентації даної галузі та підходів до захисту інформації. На основі результатів аналізу відповідної нормативно-правової документації було встановлено, що вона не є достатньою для роз’язання задач забезпечення інформаційної безпеки.

Побудована матрична модель системи захисту інформації в хмарних СКБД базується на вимогах законодавста до захисту інформації відповідно до її класифікації, вимогах міжнародних стандартів ISO/IEC щодо захисту інформації, проведеному аналізі актуальних вразливостей, загроз та застосовних заходів безпеки. Також проведено аналіз існуючих засобів захисту для кожного з аспектів, та їх пріоритизацію.

Таким чином, дана модель забезпечує повне покриття питань захисту інформації в хмарних системах керування базами даних, при цьому обгрунтованість використання визначених контролів є абсолютно прозорою для косристувача. Провайдери хмарних сервісів (як ті, що тільки виходять на ринок, так і досвідчені суб’єкти ринку), які прагнуть покращити систему захисту інформаційних активів, забезпечити повне покриття питань захисту інформації та вести свою дяільність у відповідності до міжнародних стандартів можуть використовувати дану модель для посудови СЗІ.

4 АНАЛІЗ ВИХОДУ НА РИНОК СТАРТАП ПРОЕКТУ

4.1 Опис ідеї стартап проекту

Таблиця 4.1 – Опис ідеї стартап-проекту

Зміст ідеї	*Напрямки застосування*	*Вигоди для користувача*
До викорастання провайдерам хмарних сервісів та їх споживачам пропонується модель системи захисту інформації в хмарних СКБД. Модель представлена у матричному вигляді, та побудована на множинах: вразливостей, загроз, агентів загроз, контролів та рекомендацій щодо їх використання. Дана модель пропонує повне покриття питання захисту сновних властивостей інформації (конфіденційності, цілісності та доступності) в хмарних СКБД та забезпечує оптимальність використання ресурсів для засисту інформації та прозорість їхнього застосування у відношенні покриття питань ІБ, що базуються на парах вразливостей та загроз.	1. Використання моделі провайдерами хмарних СКБД	1. Забезпечення повного покриття питань захисту інформації та оптимізації використання ресурсів для захисту інформації. 2. Забезпечення прозорості покриття питань захисту інформації відповідними контролями. 3. Використання актуальних рекомендацій стосовно засобів захисту інформації в хмарних СКБД.
	2. Використання моделі користувачами хмарних СКБД.	1. Забезпечення розуміння (надання вичерпної інформації) аспектів інформаційної безпеки своїх ресурсів та забезпечення можливості врахувати усі необхідні пункти при укладанні договорів з постачальниками послуг.

Таблиця 4.2 – Визначення сильних, слабких та нейтральних характеристик ідеї проекту

№ п/п	*Техніко-економічні характеристики ідеї*	*(Потенційні) товари/концепції конкурентів*				*W (слабка сторона)*	*N (нейтральна сторона)*	*S (сильна сторона)*
		Мій проект	*Конкурент1*	*Конкурент2*	*Конкурент3*			
1	2	3	4	5	6	7	8	9
1.	Покриття питань захисту інформації і хмарних СКБД та оптимізація використання ресурсів захисту.	Забезпечення повного покриття питань захисту інформації та оптимізації використання ресурсів для захисту інформації.	Забезпечення захисту інформації в системі «під ключ», забезпечує замовника інструментом для здійснення повного контролю за інформаційними активами, але хмарні сервіси не є профільним напрямком конкурента	Надання консультативних послуг в галузі забезпечення інформаційнох безпеки.	Аудиторські послуги та проведення тестування на проникнення.	Надання лише консультативних послуг та рекомендація деяких з тих інструментів, що знаходяться у відкритому доступі	– Модель повністю адаптована для захисту інформації в хмарних СКБД; – Надання рекомендацій з питань захисту інформаційної безпеки, які є актуальними та можуть бути частково виористані і для інших систем.	– Повне покриття питання інформаційної безпеки; – Модель повністю адаптована для захисту інформації в хмарних СКБД.
2.	Прозорість використання відповідних контролів для	Забезпечення повної прозорості покриття.	Відсутність прозорості покриття питань	Надання консультативних послуг,	Надання консультативних послуг, без впровадження.	Відповідальність за впровадження контролів	Забезпечення прозорості використання контролів.	Забезпечення повної прозорості використання

Продовження таблиці 4.2

1	2	3	4	5	6	7	8	9
	захисту інформації.	питань захисту інформації відповідними контролями та доцільності їхнього використання	захисту інформації відповідними контролями та доцільності їхнього використання; не орієнтовано на хмарні сервіси.	без впровадження заходів та засобів забезпечення інформаційної безпеки; не орієнтовано на хмарні сервіси.	заходів та засобів забезпечення інформаційної безпеки; не орієнтовано на хмарні сервіси	лежить на замовнику.		контролів у відповідності до потенційних врзливостей та загроз, в розрізі хмарних сервісів та надання найактуальніших рекомендацій щодо контролів та їх впровадження.
3.	Актуальність рекомендацій стосовно використання засобів захисту інформації в хмарних СКБД.	Надання найактуальніших рекоменцій та консультативних послуг стосовно використання засобів захисту інформації в хмарних СКБД.	Відсутність консультативних та рекомендодавчих послуг; не орієнтовано на хмарні сервіси.	Надання консультативних послуг; не орієнтовано на хмарні сервіси.	Надання лише певного визначеного обсягу консультативних послуг, що базуються на результатах проведеного аудиту та \ або результатах тестування на проникнення; не орієнтовано	Модель системи захисту потребує неперервного процесу оновлення згідно зі змінами в законодавстві, міжнародних стандартах, а також в зв’язку з динамічністю.	Усі послуги, що надаються в галузі інформаційної безпеки потребують неперервного процесу актуалізації, інакше унеможливлюється забезпечення належного рівня захисту	Модель системи захисту інформації забезпечує найактуальніші рекомендації стосовно використання засобів захисту інформації в хмарних СКБД завдяки наявності неперервного

Продовження таблиці 4.2

1	2	3	4	5	6	7	8	9
					на хмарні сервіси.	виникнення нових загроз в галузі інформаційної безпеки та відповідно до вимог клієнта	інформації в кіберпросторі.	процесу відслідковування змін в законодавстві, міжнародних стандартах, а також динаміки виникнення нових загроз в галузі інформаційної безпеки та відповідно до вимог клієнта.
4.	Вичерпність інформації стосовно аспектів інформаційної безпеки	Надання максимально вичерпної і актуальної інформації та консультативних послуг стосовно використання засобів захисту інформації в хмарних СКБД.	Надання вичерпної інформації щодо системи захисту може бути передбачено умовами договору з клієнтом.	Послуги даного конкурента базуються на наданні консультативних послуг, отже, інформація має бути актуальною та вичерпною, якщо	Надання лише певного визначеного обсягу консультативних послуг, що базуються на результатах проведеного аудиту та \ або результатах тестування на проникнення.	Необхідність неперервного процесу актуалізації інформації.	Надання вичерної інформації стосовно аспектів захисту інформації в хмарних СКБД.	Модель системи захисту інформації забезпечує надання вичерпних рекомендацій стосовно використання засобів захисту інформації в хмарних СКБД завдяки наявності неперервного

Продовження таблиці 4.2

1	2	3	4	5	6	7	8	9
				іншого не передбачено умовами договору або іншими регламентуючими документами.				процесу оновлення.

4.2 Технологічний аудит ідеї проекту

Таблиця 4.3 – Технологічна здійсненність ідеї проекту

№ п/п	*Ідея проекту*	*Технології її реалізації*	*Наявність технологій*	*Доступність технологій*
1	2	3	4	5
1.	Модель системи захисту інформації в хмарних СКБД, що забезпечує повне покриття	Для впровадження даного проекту необхідно: 1. Найняти команду технічних спеціалістів для	Технології є доступними та стосуються виключно найму персоналу або передачі певного виду робіт на аутсорсинг.	Технологія є доступною

Продовження таблиці 4.3

1	2	3	4	5
	питань захисту інфомації в даній галузі. Представлена у матричному вигляді та пропонується до використання в рамках надання консультативних послуг.	забезпечення підтримки та актуалізації моделі 2. Найняти команду технічних спеціалістів для надання консультативних послуг		
		3. Найняти або користуватись послугами юриста\групи юристів для відслідковування змін в законодавстві на інших нормативно-правових документах, а також надання інших юридичних послуг, що стосуються	Технології є доступними та стосуються виключно найму персоналу або передачі певного виду робіт на аутсорсинг.	Технологія є доступною

Продовження таблиці 4.3

1	2	3	4	5
		реалізації проекту		
		4. Найняти персонал або віддати на аутсорсинг інші послуги, які стосуються реалізації проекту	Технології є доступними та стосуються виключно найму персоналу або передачі певного виду робіт на аутсорсинг.	Технологія є доступною
1. Обрана технологія реалізації ідеї проекту: • Найняти команду технічних спеціалістів для забезпечення підтримки та актуалізації моделі • Найняти команду технічних спеціалістів для надання консультативних послуг • Найняти або користуватись послугами юриста\групи юристів для відслідковування змін в законодавстві на інших нормативно-правових документах, а також надання інших юридичних послуг, що стосуються реалізації проекту • Найняти персонал або віддати на аутсорсинг інші послуги, які стосуються реалізації проекту				

За результатами аналізу, наведеного вище, було встановлено, що даний проект є технічно реалізовним. Оскільки для реалізації необхідно лише найняти вищевказаний персонал з відповідним рівнем кваліфікації у вищевказаних питаннях, то стратегією до реалізації цього завдання обрано проведення ряду інтерв'ю з кандидатами та формування команд, аналіз

доцільності передачі певних процесів на аутсорсинг та, відповідно, передача пених процесів на аутсорсинг або найм персоналу для виконання їх всередині компанії.

4.3 Аналіз ринкових можливостей запуску стартап проекту

Таблиця 4.4 – Попередня характеристика потенційного ринку стартап-проекту

№ п/п	*Показники стану ринку (найменування)*	*Характеристика*
1	Кількість головних гравців, од	30
2	Загальний обсяг продаж, грн/ум.од	15 000
3	Динаміка ринку (якісна оцінка)	Зростає
4	Наявність обмежень для входу (вказати характер обмежень)	Необхідність початкового капіталу та наявність конкуренції
5	Специфічні вимоги до стандартизації та сертифікації	Стандартизація та сертифікація проводиться у відповідності до стандартів ISO: ISO/IEC 27001 «Інформаційні технології - Методи забезпечення безпеки - Системи управління інформаційною безпекою - Вимоги».
6	Середня норма рентабельності в галузі (або по ринку), %	Рентабельність проекту складає 123%, що є вищим за показник рентабельності банківського вкладу на 8-11%. Розрахунки наведено нижче.

Отже, як видно з висченаведених розрахунків, рентабельність проекту складає 123%, що є вищим за показник рентабельності банківського вкладу на 8-11%, тому реалізація даного проекту є економічно вигідною.

4.4 Розроблення маркетингової програми

Таблиця 4.5 – Характеристика потенційних клієнтів стартап-проекту

№ п/п	*Потреба, що формує ринок*	*Цільова аудиторія (цільові сегменти ринку)*	*Відмінності у поведінці різних потенційних цільових груп клієнтів*	*Вимоги споживачів до товару*
1	2	3	4	5
1.	– Потреба в повній та вичерпній моделі для побудови системи захисту інформації в хмарних СКБД, а також переліку рекомендацій стосовно впровадження необхідних контролем з роз'ясненням того, як саме дані контролі покривають питання інформаційної безпеки. – Необхідність сертифікації СУІБ відповідно до вищевказаних міжнародних стандартів.	– Провайдери хмарних сервісів (як ті, що тільки виходять на ринок, так і досвідчені суб'єкти ринку), які прагнуть покращити систему захисту інформаційних активів, забезпечити повне покриття питань захисту інформації та вести свою діяльність у відповідності до міжнародних стандартів. – Користувачі хмарних сервісів, які прагнуть прозорості у питаннях захисту інформації, можуть переконатись, що постачальник забезпечує належний рівень захисту інформаційних ресурсів, а	– Дану галузь регламентує законодавство\ва країн\ни, та міжнародні стандарти ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005, ISO/IEC 17788, ISO/IEC 17789, GDPR; – Підвищення рівня стурбованності питаннями інформаційної безпеки; – Необхідність сертифікації СУІБ відповідно до вищевказаних міжнародних стандартів.	– Отримання консультативних послуг в питаннях систем захисту інформації в хмарних СКБД; – Універсальність та повнота матричної моделі системи захисту інформації; – Оптимізація ресурсів, спрямованих на забезпечення інформаційної безпеки; – Прозорість покриття контролями питань інформаційної безпеки.

Продовження таблиці 4.5

1	2	3	4	5
		також для розуміння розподілу відповідальності за забезпечення належного рівня безпеки та адміністравання СКБД між користувачем та постачальником хмарних послуг (в тому числі, розуміння того, як грамотно скласти договір з постачальником).		

Таблиця 4.6 – Фактори загроз

№ п/п	*Фактор*	*Зміст загрози*	*Можлива реакція компанії*
1	2	3	4
1.	Недостатня інформованість суспільства щодо питань інформаційної безпеки та необхідності побудови систем захисту інформації	Потенційні користувачі нехтують питаннями забезпечення захисту інформації через недостатню обізнаність в галузі інормаційної безпеки і, як наслідок, неусвідомлення криточності інформаційних активів та можливих наслідків для організації; вразливостей та загроз, застосовних до систем, в яких проводиться обробка та/або зберігання інформації і каналів її передачі.	Підвищувати інформованість суспільства стосовно питань інформаційної безпеки, брати участь у різноматних конференціях та подібних заходах, поширення інформації за допомогою соціальних мереж та публікації статей, що мають просвітницький характер; кооперуватись з постачальниками хмарних послуг, інформаційних технологій та засобів захисту інформації для взаємного отримання вигоди в наслідок дяльності цієї кооперації.

Продовження таблиці 4.6

1	2	3	4
2.	Недостатність стартового капіталу	Неможливість подолання бар'єру виходу на ринок через недостатність стартового капіталу.	Залучення інвесторів, які отримуватимуть певний відсоток майбутього прибутку.
3.	Наявність конкуренції	Неможливість подолання бар'єру виходу на ринок через велику конкуренцію в галузі.	Орієнтація на здобуття конкурентої переваги шляхом покращення якості надання послуг а також через те, що дана модель створена та адаптована для хмарних СКБД, в той час як більшість моделей стосуються інформаційних систем в цілому.

Таблиця 4.7 – Фактори можливостей

№ п/п	*Фактор*	*Зміст можливості*	*Можлива реакція компанії*
1.	Необхідність забезпечення належного рівня захисту даних в хмарних СКБД відповідно до діючого законодавства та міжнародних стандартів	Модель створено на основі вимог міжнародних стандартів та відповідного діючого законодавствав сфері захисту інформації, а також орієнтовано на хмарні СКБД, що огрунтовує можливість виходу даного проекту на ринок.	Забезпечення та підтримання виского рівня надання послуг, завдяки наявності процесу відслідковування змін в законодавстві та міжнародних стандартах, постійній актуалізації моделі реагуючи на події в кіберпросторі.
2.	Необхідність сертифікації СУІБ відповідно до вищевказаних міжнародних стандартів	В зв'язку з необхідністю сертифікації СУІБ зростає попит на консультативні послуги та послуги впровадження ІБ в даній галузі. Модель створено на основі вимог міжнародних стандартів, що , як наслідок, передбачає відповідність даним вимогам.	Забезпечення та підтримання виского рівня надання послуг, завдяки наявності процесу відслідковування змін в міжнародних стандартах та актуалізація моделі у відповідності до внесених змін.
3.	Підвищення рівня стурбованності питаннями інформаційної безпеки	Внаслідок глобальної інформатизації, рівень критичності інформаційних активів для організації набуває найвищого значення з	Розповсюдження інформації щодо важливості питань інформаційної безпеки вищевказаними методами.

		точки зору впливу на бізнес, та, головне – досягнення організацією її цілей, що є основним показником ефективності.	

Таблиця 4.8. Ступеневий аналіз конкуренції на ринку

Особливості конкурентного середовища	*В чому проявляється дана характеристика*	*Вплив на діяльність підприємства (можливі дії компанії, щоб бути конкурентоспроможною)*
1	2	3
1. Тип конкуренції - чиста	Конкуренція характерна для галузі з низьким ступенем монополізації	Забезпечення більш високого рівня надання консультативних послуг за рахунок постійної актуалізації моделі, прозорості використання засобів безпеки та певним визначеним напрямком, орієнтованим на хмарні сервіси.
2. За рівнем конкурентної боротьби - національний	Конкурентна боротьба в межах визначеної країни	Забезпечення більш високого рівня надання консультативних послуг за рахунок постійної актуалізації моделі, прозорості використання засобів безпеки та певним визначеним напрямком, орієнтованим на хмарні сервіси.
3. За галузевою ознакою - внутрішньогалузева	Конкуренція в межах галузі	Забезпечення більш високого рівня надання консультативних послуг за рахунок постійної актуалізації моделі, прозорості використання засобів безпеки та певним визначеним напрямком, орієнтованим на хмарні сервіси.
4. Конкуренція за видами товарів: - товарно-родова	Товарно-родова - конкуренція між різними видами товарів, які можуть виконувати подібні	Забезпечення більш високого рівня надання консультативних послуг за рахунок постійної актуалізації моделі,

Продовження таблиці 4.8

1	2	3
	функції. Мається на увазі конкуренція з боку товарів-субститутів (замінників).	прозорості використання засобів безпеки та певним визначеним напрямком, орієнтованим на хмарні сервіси.
5. За характером конкурентних переваг - нецінова	Конкуренція за рахунок покращення якості надаваних послуг	Забезпечення більш високого рівня надання консультативних послуг за рахунок постійної актуалізації моделі, прозорості використання засобів безпеки та певним визначеним напрямком, орієнтованим на хмарні сервіси.
6. За інтенсивністю - не марочна	Відсутня необхідність випуску ряду товарів під однією маркою	Забезпечення більш високого рівня надання консультативних послуг за рахунок постійної актуалізації моделі, прозорості використання засобів безпеки та певним визначеним напрямком, орієнтованим на хмарні сервіси.

Таблиця 4.9 – Аналіз конкуренції в галузі за М. Портером

Складові аналізу	*Прямі конкуренти в галузі*	*Потенційні конкуренти*	*Постачальники*	*Клієнти*	*Товари-замінники*
1	2	3	4	5	6
	Навести перелік прямих конкурентів	– Недостатня інформованість суспільства щодо питань інформаційної безпеки та необхідності		Дана послуга є дедалі більш необхідною в умовах переходу до використання хмарних сервісів; клієнти не чинять впливу на умови роботи на ринку, але можуть	Фактори загроз з боку зоку товарів-субститутів полягають в тому, що користувачі даної послуги можуть обирати між пропозиціями базуючись на власних знаннях та на рекламних компаніях. Пир цьому

Продовження таблиці 4.9

1	2	3	4	5	6
		побудови систем захисту інформації – Недостатність стартового капіталу – Наявність конкуренції	В зв’язку зі специфікою роботи питання про вплив зі сторони постачальників не є застосовним.	створювати певний попит відносно до ступеня їх обізнаності в питаннях інформаційної безпеки та розуміння необхідності впровадження систем захисту.	користувач може необ’єктивно оцінити послугу з огляду на недостатність вхідної інформації або її неактульність, а також через відстуність розуміння того, що саме очікується від надаваємої послуги, а також як трактувати результати проведеної роботи. Так як, наприклад, модель орієнтовано на системи захисту інформації в хманих СКБД і диференціація критичності визначеного переліку засобів безпеки є дещо іншою, ніж для систем, на які орієнтовано послуги компаній-конкурентів.
Висновки:		– Можливості виходу на ринок є та обгрунтовані рентабельністю проекту, попитом, створеним за разунок підвищення рівня стурбованності суспільства	В зв’язку зі специфікою роботи питання про контроль умов роботи на ринку зі сторони	Дана послуга є дедалі більш необхідною в умовах переходу до використання хмарних сервісів; клієнти не чинять впливу на умови роботи на ринку, але можуть створювати певний попит відносно до ступеня їх обізнаності в питаннях інформаційної безпеки та розуміння необхідності	В зв’язку зі специфікою роботи питання про обмеження роботи на ринку зі сторони товарів-субститів не є застосовним.

Продовження таблиці 4.9

1	2	3	4	5	6
	Конкуренція в галузі надання консультативних послуг з інформаційної безпеки на національному рівні не є досить високою. Великі компанії-конкуренти займаються суміжними питаннями безпеки,тому вихід проекту на ринок не буде суттєво ускладнено питаннями конкуренції.	питаннями інформаційної безпеки; необхідністю сертифікації СУІБ відповідно до вищевказаних міжнародних стандартів. – В зв’язку зі специфікою роботи питання про потенційну конкуренцію не є актуальним.	постачальників не є застосовним.	впровадження систем захисту.	

Таблиця 4.10 – Обґрунтування факторів конкурентоспроможності

№ п/п	*Фактор конкурентоспроможності*	*Обґрунтування (наведення чинників, що роблять фактор для порівняння конкурентних проектів значущим)*
1.	Покриття питань захисту інформації і хмарних СКБД та оптимізація використання ресурсів захисту інформації	Забезпечення повного покриття питань захисту інформації та оптимізації використання ресурсів для захисту інформації
2.	Прозорість використання відповідних контролів для захисту інформації	Забезпечення повної прозорості покриття питань захисту інформації відповідними контролями та доцільності їхнього використання
3.	Актуальність рекомендацій стосовно використання засобів захисту інформації в хмарних СКБД	Надання найактуальніших рекоменцій та консультативних послуг стосовно використання засобів захисту інформації в хмарних СКБД
4.	Вичерпність інформації стосовно аспектів інформаційної безпеки	Надання максимально вичерпної і актуальної інформації та консультативних послуг стосовно використання засобів захисту інформації в хмарних СКБД

Таблиця 4.1 – Порівняльний аналіз сильних та слабких сторін «назва проекту»

№ п/п	*Фактор конкурентоспроможності*	*Бали 1-20*	*Рейтинг товарів-конкурентів у порівнянні з даним проектом*						
			–3	*–2*	*–1*	*0*	*+1*	*+2*	*+3*
1.	Покриття питань захисту інформації і хмарних СКБД та оптимізація використання ресурсів захисту.	18		+					
2.	Прозорість використання відповідних контролів для захисту інформації.	20		+					
3.	Актуальність рекомендацій стосовно використання засобів захисту інформації в хмарних СКБД.	19-20				+			
4.	Вичерпність інформації стосовно аспектів інформаційної безпеки	19-20				+			

Таблиця 4.2 – SWOT- аналіз стартап-проекту

Сильні сторони: • Покриття питань захисту інформації і хмарних СКБД та оптимізація використання ресурсів захисту. • Прозорість використання відповідних контролів для захисту інформації. • Актуальність рекомендацій стосовно використання засобів захисту інформації в хмарних СКБД. • Модель повністю адаптована для захисту інформації в хмарних СКБД. • Вичерпність інформації стосовно аспектів інформаційної безпеки.	Слабкі сторони: • Надання лише консультативних послуг та рекомендація деяких з тих інструментів, що знаходяться у відкритому доступі. • Відповідальність за впровадження контролів лежить на замовнику. • Модель системи захисту потребує неперервного процесу оновлення згідно зі змінами в законодавстві, міжнародних стандартах, а також в зв’язку з динамічністю виникнення нових загроз в галузі інформаційної безпеки та відповідно до вимог клієнта. • Необхідність неперервного процесу актуалізації інформації.
Можливості: • Необхідність забезпечення належного рівня захисту даних в хмарних СКБД відповідно до діючого законодавства та міжнародних стандартів. • Необхідність сертифікації СУІБ відповідно до вищевказаних міжнародних стандартів. • Підвищення рівня стурбованності питаннями інформаційної безпеки.	Загрози: • Недостатня інформованість суспільства щодо питань інформаційної безпеки та необхідності побудови систем захисту інформації. • Недостатність стартового капіталу. • Наявність конкуренції.

Таблиця 4.3 – Альтернативи ринкового впровадження стартап-проекту

№ п/п	*Альтернатива (орієнтовний комплекс заходів) ринкової поведінки*	*Ймовірність отримання ресурсів*	*Строки реалізації*
1.	Підвищувати інформованість суспільства стосовно питань інформаційної безпеки, брати участь у різноматних конференціях та подібних заходах, поширення інформації за допомогою соціальних мереж та публікації статей, що мають просвітницький характер; кооперуватись з постачальниками хмарних послуг, інформаційних технологій та засобів захисту інформації для взаємного отримання вигоди в наслідок дяльності цієї кооперації. Орієнтація на здобуття конкурентої переваги шляхом покращення якості надання послуг а також через те, що дана модель створена та адаптована для хмарних СКБД, в той час як більшість моделей стосуються інформаційних систем в цілому.	Орієнтація на здобуття конкурентої переваги шляхом покращення якості надання послуг а також через те, що дана модель створена та адаптована для хмарних СКБД, в той час як більшість моделей стосуються інформаційних систем в цілому.	3-5 місяців

4.5 Розроблення ринкової стратегії проекту

Таблиця 4.4 – Вибір цільових груп потенційних споживачів

№ п/п	*Опис профілю цільової групи потенційних клієнтів*	*Готовність споживачів сприйняти продукт*	*Орієнтовний попит в межах цільової групи (сегменту)*	*Інтенсивність конкуренції в сегменті*	*Простота входу у сегмент*
1	2	3	4	5	6
1.	Провайдери хмарних сервісів (як ті, що тільки виходять на				

Продавження таблиці 4.14

1	2	3	4	5	6
	ринок, так і досвідчені суб’єкти ринку), які прагнуть покращити систему захисту інформаційних активів, забезпечити повне покриття питань захисту інформації та вести свою діяльність у відповідності до міжнародних стандартів.				
2.	Користувачі хмарних сервісів, які прагнуть прозорості у питаннях захисту інформації, переконатись, що постачальник забезпечує належний рівень захисту інформаційних ресурсів, а також для розуміння розподілу відповідальності за забезпечення належного рівня безпеки та адміністравання СКБД між користувачем та постачальником хмарних послуг (в тому числі, розуміння того, як грамотно скласти договір з постачальником).				
Які цільові групи обрано: провайдери хмарних сервісів; користувачі хмарних сервісів.					

Таблиця 4.5 – Визначення базової стратегії розвитку

№ п/п	*Обрана альтернатива розвитку проекту*	*Стратегія охоплення ринку*	*Ключові конкурентоспроможні позиції відповідно до обраної альтернативи*	*Базова стратегія розвитку*
1.	Популяризація питань ІБ (публікації статей, участь у конференціях); Кооперування з більш відомими компаніями з метою отримання взаємовигідних результатів.			

Таблиця 4.6 – Визначення базової стратегії конкурентної поведінки

№ п/п	*Чи є проект «першопрохідцем» на ринку?*	*Чи буде компанія шукати нових споживачів, або забирати існуючих у конкурентів?*	*Чи буде компанія копіювати основні характеристики товару конкурента, і які?*	*Стратегія конкурентної поведінки*
1.	Дана послуга не являється першопрохідцем на ринку, існує ряд суміжних послуг. Проте, даний проект має ряд унікальних властивостей, зокрема адаптованість до хмарних сервісів.	Передбачується утворення власного кола споживачів, оскільки модель орієнтована на певну визначену аудиторію; при цьому не можна виключати того, що частина споживачів перейде від конкурентів за	Цей пункт є застосовним лише до процесів забезпечення якості послуги, наприклад неперевного моніторингу та оновлення,	Створення власного кола споживачів, чя діяльність базується на хмарних сервісах.

		рахунок більш профільного підходу та ряду якісних переваг.		

Таблиця 4.7 – Визначення стратегії позиціонування

№ п/п	*Вимоги до товару цільової аудиторії*	*Базова стратегія розвитку*	*Ключові конкурентоспроможні позиції власного стартап-проекту*	*Вибір асоціацій, які мають сформувати комплексну позицію власного проекту (три ключових)*

4.6 Розроблення маркетингової програми стартап-проекту

Першим кроком є формування маркетингової концепції товару, який отримає споживач. Для цього у табл. 18 потрібно підсумувати результати попереднього аналізу конкурентоспроможності товару.

Таблиця 4.8 – Визначення ключових переваг концепції потенційного товару

№ п/п	*Потреба*	*Вигода, яку пропонує товар*	*Ключові переваги перед конкурентами (існуючі або такі, що потрібно створити*
1.	Потреба в повній та вичерпній моделі для побудови системи захисту інформації в хмарних СКБД, а також переліку рекомендацій стосовно впровадження необхідних контролем з роз’ясненням того, як саме дані контролі покривають питання інформаційної безпеки	Забезпечення повного покриття питань захисту інформації та оптимізації використання ресурсів для захисту інформації, а також надання максимально вичерпної і актуальної інформації та консультативних послуг стосовно використання	Забезпечується повне покриття питання інформаційної безпеки; Модель повністю адаптована для захисту інформації в хмарних СКБД.

		засобів захисту інформації в хмарних СКБД	
2.	Необхідність сертифікації СУІБ відповідно до вищевказаних міжнародних стандартів	В зв'язку з необхідністю сертифікації СУІБ зростає попит на консультативні послуги та послуги впровадження ІБ в даній галузі. Модель створено на основі вимог міжнародних стандартів, що , як наслідок, передбачає відповідність даним вимогам.	Забезпечення та підтримання виского рівня надання послуг, завдяки наявності процесу відслідковування змін в міжнародних стандартах та актуалізація моделі у відповідності до внесених змін.

Надалі розробляється трирівнева маркетингова модель товару: уточнюється ідея продукту та/або послуги, його фізичні складові, особливості процесу його надання (табл. 19). Орієнтовний перелік можливих характеристик товару наведено у додатку С.

Таблиця 4.9 – Опис трьох рівнів моделі товару

Рівні товару	*Сутність та складові*		
I. Товар за задумом	Опис базової потреби споживача, яку задовольняє товар (згідно концепції), її основної функціональної вигоди		
II. Товар у реальному виконанні	Властивості/характеристики	М/Нм	Вр/Тх /Тл/Е/Ор
	1. ….. 2. ……		
	Якість: стандарти, нормативи, параметри тестування тощо		
	Пакування		
	Марка: назва організації-розробника + назва товару		
III. Товар із підкріпленням	До продажу		
	Після продажу		
За рахунок чого потенційний товар буде захищено від копіювання: в зв'язку зі специфікою надання послуг питання про захист від копіювання не є застосовним.			

Таблиця 4.10 – Визначення меж встановлення ціни

№ п/п	*Рівень цін на товари-замінники*	*Рівень цін на товари-аналоги*	*Рівень доходів цільової групи споживачів*	*Верхня та нижня межі встановлення ціни на товар/послугу*

Таблиця 4.11 – Формування системи збуту

№ п/п	*Специфіка закупівельної поведінки цільових клієнтів*	*Функції збуту, які має виконувати постачальник товару*	*Глибина каналу збуту*	*Оптимальна система збуту*

Таблиця 4.12. – Концепція маркетингових комунікацій

№ п/п	*Специфіка поведінки цільових клієнтів*	*Канали комунікацій, якими користуються цільові клієнти*	*Ключові позиції, обрані для позиціонування*	*Завдання рекламного повідомлення*	*Концепція рекламного звернення*

ПЕРЕЛІК ПОСИЛАНЬ

1. ISO/IEC 17788 – 2014. Information technology – Cloud computing – Overview and vocabulary. – Publ. 2014-10-15. – Geneva: ISO, 2014. – 10 p.
2. NIST Special Publication 800-39, Managing Information Security Risk. Organization, Mission, and Information System View. Information security. – 2011. http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf
3. ПРО ЗАТВЕРДЖЕННЯ Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах: постанова Кабінету Міністрів України від 29.03.2006 р. № 373 // Законодавчі та нормативні документи України у сфері інформації, видавничої та бібліотечної справи: темат. Добірка. - К., 2007. - Ч.1. - С.74-77.
4. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994 № 80/94-ВР.
5. Закон України «Про захист персональних даних»;
6. Закон України «Про доступ до публічної інформації»;
7. Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах (Постанова Кабінету Міністрів України від 29.03.06 № 373);
8. Концепція технічного захисту інформації в Україні (Постанова Кабінету Міністрів України від 8.10.97 №1126);
9. Положення про технічний захист інформації в Україні (Указ Президента України від 27.09.99 № 1229/99).

10. НД ТЗІ 3.7-003-05 "Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі"